UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

METODOLOGÍA BASADA EN EL CÓMPUTO FORENSE PARA LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

DEMIAN ROBERTO GARCÍA VELÁZQUEZ

DIRECTORA:

M.C. MA. JAQUELINA LÓPEZ BARRIENTOS

MÉXICO, D.F. ABRIL 2014

Índice

Introducción. i
Objetivo General iii
Objetivos Particulares iv
Capítulo 1 Delitos Informáticos 2
1.1. Definición de delito informático 4
1.2. Tipos de delitos informáticos. 9
1.3. Los delitos informáticos en la legislación mexicana. 14
1.3.1. Clasificación de los delitos informáticos en la legislación mexicana. 21
1.3.2. Propuesta de clasificación para la legislación mexicana. 23
1.4. Elección y justificación de los delitos informáticos a utilizar 29
Capítulo 2 Cómputo Forense 32
2.1. Introducción al cómputo forense. 33
2.2. La evidencia digital. 39
2.2.1. Tipos de evidencia. 41
2.2.2. Características de la evidencia. 43
2.3. Principales fases del cómputo forense 44
2.3.1. Identificación. 45
2.3.2. Preservación. 48
2.3.3. Análisis. 50
2.3.4. Presentación. 56
2.4. El cómputo forense como herramienta para la persecución del delito. 59
Capítulo 3 Metodología para la investigación de delitos informáticos con base en el cómputo forense 61
3.1. Generalidades de la metodología. 62
3.2. Una metodología para redes LAN. 64
3.3. Metodología propuesta. 66

3.3.1. Proceso de preparación. 67
3.3.2 Proceso de identificación. 70
3.3.3. Proceso de preservación. 78
3.3.4. Proceso de análisis. 83
3.3.5. Proceso de presentación. 87
Capítulo 4 Ambientes controlados para la implementación de la metodología. 90
4.1. Uso de ambientes controlados. 92
4.2. Características de los escenarios a investigar en ambientes controlados. 93
4.3. Descripción del Caso A. 98
4.4. Descripción del Caso B. 99
4.5. Detalles técnicos para los Casos A y B. 100
Capítulo 5 Implementación y resultados de la metodología en el Caso A. 105
5.1. Etapa de preparación. 106
5.2. Etapa de identificación. 108
5.3. Etapa de preservación. 116
5.4. Etapa de análisis. 120
5.5. Etapa de presentación. 126
Capítulo 6 Implementación y resultados de la metodología en el Caso B. 136
6.1. Etapa de preparación. 137
6.2. Etapa de identificación. 139
6.3. Análisis en vivo. 147
6.3.1. Procesos en ejecución. 147
6.3.2. Conexiones establecidas. 149
6.3.3. Volcado y análisis de memoria RAM. 152
6.4. Análisis básico de malware. 164
6.4.1. Paso 1. Creación de un ambiente virtual. 165
6.4.2. Paso 2. Documentación del estado del sistema recién instalado. 165
6.4.3. Paso 3. Infección del sistema virtual. 167
6.4.4. Paso 4. Documentación del estado del sistema infectado. 168
6.4.5. Paso 5. Conclusiones del análisis básico de malware. 171
6.5. Etapa de identificación, sistema detenido uno. 172
6.6. Etapa de preservación, sistema detenido uno. 174

6.7. Etapa de análisis, sistema detenido uno. 178
6.8. Etapa de identificación, sistema detenido dos. 187
6.9. Etapa de preservación, sistema detenido dos. 192
6.10. Etapa de análisis, sistema detenido dos. 196
6.11. Etapa de presentación. 207
Conclusiones 223
Anexo I 229
Glosario 233
Bibliografía y referencias de Internet. 238

Índice de Figuras

Figura 1.1 Sujetos de la cadena de interacciones 5
Figura 1.2 Cadena de interacciones 6
Figura 1.3 Keylogger físico. 12
Figura 2.1 Etapas del método científico. 35
Figura 4.1 Ataques por tamaño de la organización objetivo. 95
Figura 4.2 Distribución de sistemas operativos según Net Market Share 101
Figura 4.3 Distribución de sistemas operativos según StatCounter. 102
Figura 5.1 Interfaz principal de FTK Imager. 117
Figura 5.2 Selección de tipo de dispositivo origen. 118
Figura 5.3 Selección del destino de la imagen y tamaño de los fragmentos. 119
Figura 5.4 Evidencia, archivo tipo imagen. 120
Figura 5.5 Evidencia correctamente montada. 121
Figura 5.6 Contenido del directorio de Microsoft Outlook. 122
Figura 5.7 Exportación del archivo Outlook.pst. 122
Figura 5.8 Hash MD5 del archivo Outlook.pst. 123
Figura 5.9 Interfaz de PSTViwer Pro 4. 124
Figura 5.10 Contenido del archivo “Datos Pacientes.xlsx”. 125
Figura 5.11 Registros de correo electrónico en la imagen forense. 130
Figura 5.12 Extracción de registros de correo electrónico. 130
Figura 5.13 Hash MD5 del registro de correo electrónico. 131
Figura 5.14 Correos enviados por “consul-med-ac@outlook.com”. 132
Figura 5.15 Contenido del archivo “Datos Pacientes.xlsx”. 133
Figura 6.1 Procesos listados por Process Explorer. 148
Figura 6.2 Conexiones establecidas en el equipo sospechoso. 149
Figura 6.3 Propiedades del proceso services.exe 151
Figura 6.4 Interfaz de DumpIt para generar el volcado de memoria. 153

Figura 6.5Procesos alojados en memoria listados por Volatility. 156
Figura 6.6 Procesos alojados en memoria listados por Volatility. 157
Figura 6.7 Cadenas sospechosas del archivo “executable.456.exe”. 158
Figura 6.8 Análisis del archivo creado en Virus Total. 159
Figura 6.9 Resultado del análisis del ejecutable generado con Volatility. 159
Figura 6.10 Contenido del directorio de Descargas. 161
Figura 6.11 Contenido del archivo comprimido “descuentoCam.rar”. 162
Figura 6.12 Resultado del análisis de aplicación sospechosa. 162
Figura 6.13 Procesos en ejecución después de la instalación del sistema operativo. 165
Figura 6.14 Conexiones de red en el sistema recién instalado. 166
Figura 6.15 Aplicaciones legítimas ejecutadas al arranque del sistema operativo. 167
Figura 6.16 Imagen mostrada después de ejecutar la aplicación maliciosa. 167
Figura 6.17 Procesos en ejecución en el sistema infectado. 168
Figura 6.18 Conexiones de red del sistema infectado. 169
Figura 6.19 Aplicaciones ejecutadas al inicio del sistema infectado. 170
Figura 6.20 Hash MD5 para el archivo “fservice.exe” 170
Figura 6.21 Interfaz principal de FTK Imager. 175
Figura 6.22 Selección de tipo de dispositivo origen. 176
Figura 6.23 Selección del destino de la imagen y tamaño de los fragmentos. 177
Figura 6.24 Interfaz para agregar elemento de evidencia. 178
Figura 6.25 Elemento de evidencia correctamente montado 179
Figura 6.26 Archivo fservice.exe en el disco duro del sistema uno. 180
Figura 6.27 Ubicación del archivo “places.sqlite” en la imagen forense. 181
Figura 6.28 Exportar “places.sqlite” a una carpeta local. 182
Figura 6.29 Selección de archivo .sqlite para la aplicación MozillaHistoryView. 183
Figura 6.30 Interfaz de la herramienta MozillaHistoryView. 184
Figura 6.31 Descarga del archivo “descuentoCam.rar”. 184
Figura 6.32 Última modificación de la aplicación maliciosa. 185
Figura 6.33 Fechas de modificación de archivos confidenciales. 186
Figura 6.34 Ubicación del malware “fservice.exe”. 196
Figura 6.35 Hash MD5 del archivo “fserive.exe” encontrado en el equipo de Julieta Guerrero. 197
Figura 6.36 Ubicación del archivo “software” en la imagen forense. 198
Figura 6.37 Hash MD5 del archivo “software” recién extraído de la imagen forense. 199
Figura 6.38 Selección del archivo “software” para la aplicación “Registry Viewer”. 200
Figura 6.39 Entrada en el registro para la ejecución de “fservice.exe”. 200
Figura 6.40 Ubicación del archivo “History.sqlite” en la imagen forense 202
Figura 6.41 Consulta de las descargas realizadas. 204
Figura 6.42 Contenido de la carpeta predeterminada de descargas. 204
Figura 6.43 Herramienta ChromeAnalysis. 206
Figura 6.44 Visualización del correo malicioso 207
Figura 6.45 Resultado del análisis del hallazgo ANA-HED-02. 212
Figura 6.46 Resultado del análisis del hallazgo ANA-HED-03. 213
Figura 6.47 Archivo fservice.exe en el disco duro del sistema uno. 215

Figura 6.48 Ubicación del archivo “places.sqlite” en la imagen forense. 216
Figura 6.49 Descarga del archivo “descuentoCam.rar”. 216
Figura 6.50 Ubicación del malware “fservice.exe”. 218
Figura 6.51 Entrada en el registro para la ejecución de “fservice.exe”. 219
Figura 6.52 Ubicación del archivo “History.sqlite” en la imagen forense..... 219
Figura 6.53 Visualización del correo malicioso..... 220

Índice de Tablas

Tabla 1.1 Resumen del contenido de los artículos 211 bis 1 - bis 7. 16
Tabla 2.1 Procesos a realizar en la fase de identificación. 47
Tabla 2.2 Procesos de la fase de preservación..... 50
Tabla 2.3 Procesos de la fase de análisis. 55
Tabla 2.4 Tipos de informes..... 58
Tabla 3.1 Formato PREIN-APP-01. 68
Tabla 3.2 Formato: PREIN-EDA-01. 69
Tabla 3.3 Ejemplo de una carta de autorización. 70
Tabla 3.4 Ejemplo de una carta de confidencialidad. 71
Tabla 3.5 Formato IDE-EIF-01. 72
Tabla 3.6 Formato IDE-INV-01. 73
Tabla 3.7 Formato IDE-ISE-01. 73
Tabla 3.8 Formatos para activos de información. 74
Tabla 3.9 Formato PRE-CC-01. 78
Tabla 3.10 Formato LOG-CC-01. 79
Tabla 3.11 Formato PRE-GVM-01. 80
Tabla 3.12 Formato PRE-GIF-01. 81
Tabla 3.13 Formato PRE-LHA-01. 82
Tabla 3.14 Formato ANA-HED-01. 85
Tabla 4.1 Relación de software instalado en las estaciones de trabajo. 103
Tabla 5.1 Datos sobre la aplicación FTK Imager. 107
Tabla 5.2 Información sobre la esterilización del dispositivo. 108
Tabla 5.3 Información de los integrantes del equipo asignado a la investigación. 110
Tabla 5.4 Información general acerca de la investigación. 111
Tabla 5.5 Información de los empleados de la empresa afectada. 112
Tabla 5.6 Información relacionada al activo de información afectado. 113
Tabla 5.7 Información sobre el equipo que almacena el activo afectado..... 114
Tabla 5.8 Información sobre la red a la que está conectado el equipo. 115
Tabla 5.9 Información general sobre la cadena de custodia. 116
Tabla 5.10 Bitácora de acceso al dispositivo PC-09-DD01. 116
Tabla 5.11 Resumen proceso de generación de imagen forense..... 119
Tabla 5.12Información sobre el hallazgo “Outlook.pst”. 123

Tabla 5.13 Información sobre el hallazgo “Datos Pacientes.xlsx”..... 125
Tabla 5.14 Información sobre la generación de la imagen forense. 128
Tabla 5.15 Información sobre el hallazgo “Datos Pacientes.xlsx”..... 133
Tabla 6.1 Información sobre la aplicación FTK Imager. 138
Tabla 6.2 Información sobre el dispositivo esterilizado. 138
Tabla 6.3 Información de los integrantes del equipo asignado a la investigación. 142
Tabla 6.4 Información general acerca de la investigación. 142
Tabla 6.5 Información de los empleados de la empresa afectada. 144
Tabla 6.6 Información relacionada al activo de información afectado. 145
Tabla 6.7 Información sobre el equipo que almacena el activo afectado. 145
Tabla 6.8 Información sobre la red a la que está conectado el equipo. 147
Tabla 6.9 Información de las conexiones de red del proceso sospechoso. 150
Tabla 6.10 Información general relacionada con el proceso de la cadena de custodia .. 153
Tabla 6.11 Información referente a la generación del volcado de memoria. 154
Tabla 6.12 Información sobre el proceso sospechoso encontrado en memoria. 157
Tabla 6.13 Algunas aplicaciones ejecutadas por la cuenta de usuario “Administrador”.. 160
Tabla 6.14 Datos del archivo comprimido. 161
Tabla 6.15 Información sobre el hallazgo “descuentosCam.exe”. 163
Tabla 6.16 Información sobre el hallazgo “fservice.exe”. 171
Tabla 6.17 Información del activo de interés. 174
Tabla 6.18 Bitácora de acceso al dispositivo PC-01-DD01. 175
Tabla 6.19 Información referente a la generación de la imagen forense. 177
Tabla 6.20 Información sobre el hallazgo fservices.exe en el disco duro del sistema uno. 180
Tabla 6.21 Información sobre el hallazgo “places.sqlite”. 182
Tabla 6.22 Información sobre el hallazgo “descuentosCam.exe”. 185
Tabla 6.23 Información de los activos de interés. 190
Tabla 6.24 Información relacionada al dispositivo involucrado en el incidente de seguridad. 191
Tabla 6.25 Información general relacionada con el proceso de la cadena de custodia. . 193
Tabla 6.26 Bitácora para el dispositivo PC-02-DD01. 194
Tabla 6.27 Información referente a la generación de la imagen forense. 195
Tabla 6.28 Información sobre el hallazgo “fservices.exe”. 197
Tabla 6.29 Información sobre el hallazgo “software”. 199
Tabla 6.30 Información sobre el hallazgo ANA-HED-11. 201
Tabla 6.31 Documentación del hallazgo del archivo “History.sqlite”. 203
Tabla 6.32 Información del hallazgo del archivo “descuentosCam.rar”. 204
Tabla 6.33 Información sobre el hallazgo del archivo “descuentosCam.exe”. 205
Tabla 6.34 Información sobre conexiones de red del proceso sospechoso. 210
Tabla 6.35 Información referente a la generación del volcado de memoria. 211
Tabla 6.36 Información referente a la generación de la imagen forense. 214
Tabla 6.37 Información referente a la generación de la imagen forense. 217

Introducción.

Durante la década de los 90 los sistemas computacionales comenzaron a ser ampliamente utilizados en entornos muy distintos a aquellos que los vieron nacer, es decir, el uso de este tipo de sistemas no solo se veía en el campo militar o en las universidades si no que también en las oficinas de diferentes compañías que ofrecían diferentes productos o servicios. Este crecimiento exponencial fue gracias a que dichos sistemas contribuían a mejorar la productividad y la calidad de tales productos o servicios, pronto pasaron de ser una herramienta de apoyo a un artículo de primera necesidad.

Con el paso de los años, el crecimiento abrumador de Internet y la necesidad de comunicarse a lo largo y ancho del globo terráqueo convirtieron a los sistemas computacionales en un elemento indispensable para el desarrollo de toda empresa u organización. Sin importar el tipo de empresa, existe un elemento latente involucrado en el desarrollo de estas organizaciones que resulta de vital importancia al igual que los sistemas que contribuyen a este crecimiento: el activo de información.

El activo de información es la representación digital de cualquier elemento de información que tenga un valor para una organización, esta información puede ser tan “irrelevante” como la distribución de los lugares de estacionamiento o tan “sensible” como la nómina de la compañía. La información es poder.

Existe una estrecha relación entre estos dos elementos, los sistemas computacionales manejan los activos de información, ya sea transportándolos, almacenándolos o generándolos. La mayoría de las interacciones posibles con los activos de información es a través de los sistemas computacionales. Desgraciadamente los sistemas utilizados no son perfectos, simplemente son perfectibles, es por esto que la pérdida de información es un riesgo latente dentro de una organización.

Existen muchas formas de perder información, ya sea involuntariamente: daños en los equipos, accidentes, desastres naturales, entre otros o intencionalmente: robo, sabotaje, violaciones a la integridad de la información, por mencionar algunos. La pérdida de información se traduce en una pérdida de dinero, hecho intolerable para cualquier tipo de organización.

La implementación de medidas o practicas destinas a evitar la pérdida de información por alguna de estas causas puede resultar costosa y compleja según la cantidad de formas o riesgos que se pretendan evitar o disminuir.

Actualmente existen muchas acciones que atentan contra los activos de información de cualquier organización, estas acciones mal intencionadas son realizadas por diferentes personas alrededor del mundo que pueden tener, o no, un objetivo bien definido que los motiva a cometer estas acciones.

Entre los principales motivos de estas personas mal intencionadas se encuentra el dinero. Una persona puede conseguir activos de información de una organización y venderlos al mejor postor, puede conseguir datos personales y utilizarlos para realizar fraudes, puede inhabilitar parcial o totalmente a una organización como forma de protesta o utilizar la infraestructura de una organización para realizar estas actividades mal intencionadas, por mencionar algunas.

Estas actividades o prácticas pueden ser consideras como delitos, según la legislación correspondiente. En México existen leyes que contemplan estas acciones y establecen sanciones para los infractores, sin embargo aún hace falta trabajo para contemplar toda la gama de actividades malintencionadas que atentan contra los activos informáticos de las organizaciones.

Estas prácticas mal intencionadas pueden ser perseguidas para sancionar a los infractores. Para lograr este propósito es necesario realizar las investigaciones correspondientes para determinar qué fue lo que sucedió y quién es el responsable.

Para lograr este cometido existe una disciplina de la computación que se encarga del estudio de sistemas para determinar, con base en la información disponible, qué fue lo que pasó, cuándo, cómo, y quién es el responsable de las acciones que afectaron los activos de información de un sistema, esta disciplina es el cómputo forense.

El cómputo forense es una disciplina compleja que requiere de personal altamente capacitado para realizar investigaciones que sean de utilidad para una organización que se ha visto sus activos de información afectados por algún tipo de actividad malintencionada.

El contratar los servicios de este tipo de profesionales puede ser tan costoso que no es viable para cierto tipo de empresas, por ejemplo las micro, pequeñas y medianas empresas, también conocidas como MIPYMES.

Al sumar todos estos factores, las MIPYMES se encuentran en una situación altamente vulnerable debido a la incapacidad económica de proteger sus activos de información, lo que las expone a ser víctimas de alguna actividad malintencionada que pueda considerarse delito informático, además de no tener acceso a los medios necesarios para identificar a los responsables que atentan o atentaron contra sus activos de información.

Es por estos motivos que se presenta este trabajo de tesis con los siguientes objetivos:

Objetivo General:

- Desarrollar una metodología de investigación que sirva como referencia y apoyo en las investigaciones dedicadas a identificar al infractor de los delitos informáticos establecidos en el Código Penal Federal (revelación de secretos y acceso ilícito a sistemas y equipos de informática).

Objetivos Particulares:

- Desarrollar una metodología que sea accesible para pequeñas y medianas empresas.
- Implementar la metodología desarrollada en ambientes controlados para evaluar el rendimiento de la misma.
- Determinar ventajas y desventajas de la metodología propuesta.
- Contribuir al mejoramiento del Código Penal Federal al ofrecer una clasificación más extensa y completa de los diferentes delitos informáticos.

En el capítulo 1 se presenta una definición para delitos informáticos, así como un clasificación de los mismos de a cuerdo al tipo de actividades mal intencionadas que pueden realizarse para afectar a un activo de información. También se presenta el estado actual de los delitos informáticos en la legislación mexicana y se propone una nueva clasificación para este tipo de ilícitos. Finalmente se eligen los delitos a desarrollar en ambientes controlados.

El capítulo 2 expone de manera puntual el proceso del cómputo forense con sus cuatro fases principales: identificación, preservación, análisis y presentación. En cada fase se explica su importancia y cómo se lleva a cabo en el escenario actual de las investigaciones digitales. También se presenta la evidencia digital y su importancia, así como los tipos de evidencia y sus características.

El capítulo 3 presenta la metodología propuesta para la investigación de delitos informáticos basada en cómputo forense con todas las actividades a desarrollar en cada fase de la investigación. Este capítulo menciona la importancia de utilizar este tipo de herramientas y se define el enfoque y el tipo de sistemas que se contemplan para el diseño de la metodología.

En el capítulo 4 se aborda la importancia del uso de ambientes controlados para el desarrollo de pruebas que tienen por objetivo mostrar el funcionamiento de la metodología en una investigación. En este capítulo se presentan los escenarios teóricos en los que se aplica la metodología.

El capítulo 5 presenta la aplicación de la metodología en la investigación de un sistema en el que se ha presentado fuga de información confidencial y se requiere determinar cómo sucedió la extracción de datos y quién es el responsable de esta actividad. Se realizan las actividades correspondientes para el análisis de un sistema detenido.

El capítulo 6 presenta la investigación de un ambiente controlado conformado por dos sistemas afectados por espionaje industrial. La investigación de estos sistemas se lleva a cabo a través de la implementación de la metodología, realizando las actividades de análisis en vivo, análisis básico de malware y análisis de dos sistemas detenidos.

Capítulo 1

Delitos Informáticos

Hoy en día existe un gran número de personas conectadas a Internet, de acuerdo con el Instituto Nacional de Estadística y Geografía el número de internautas en nuestro país alcanzó los 46 millones de usuarios de Internet en 2013[1]. Todos estos mexicanos conectados a Internet realizan diferentes actividades en línea, ya sea participando en redes sociales, buscando información específica, enviando mensajería electrónica, jugando en línea, entre otras, y han adoptado este estilo de comunicación como propio.

Las ventajas de esta súper red de comunicación que es el Internet son amplias y diversas, algunas son: el acceso a grandes cantidades de información, mejores y más rápidas comunicaciones, grandes cantidades de entretenimiento, acceso a canales de venta y compra de bienes o servicios, nuevas vías de medios de expresión, entre muchas más. Sin embargo, Internet también tiene sus desventajas, en principio podrían parecer mucho menores en cantidad que las ventajas pero no por eso deben ser ignoradas.

Entre las desventajas que tiene Internet se encuentran los delitos informáticos. Estas actividades amenazan a los usuarios de sistemas de información de distintas formas, actualmente existe una gran cantidad de vectores de ataque que atentan contra la información de personas, empresas y gobiernos por igual.

Estas amenazas tienen alcance global gracias a Internet, lo cual las hace muy difícil de combatir, es posible que un delincuente informático se encuentre ubicado en el continente americano pero que sus actividades delictivas sean realizadas en Europa, Asia, o en cualquier parte.

En este capítulo se abordan los delitos informáticos, su definición, los diferentes tipos que existen, se muestra el panorama actual de la legislación mexicana en esta materia, y se ofrece una propuesta para mejorar la clasificación de este tipo de delitos, así mismo se plantea el uso de los delitos informáticos que se utilizan en este trabajo de investigación.

[1] http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tinf204&s=est&c=19437

[2] Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. Diccionario jurídico

1.1. Definición de delito informático

Para comprender correctamente el término “delito informático” es necesario tomar en cuenta el significado de las dos palabras que forman a dicho término. Según el diccionario jurídico mexicano, delito se define como:

> *“…acción u omisión ilícita y culpable expresamente descrita por la ley bajo la amenaza de una pena o sanción criminal”*[2].

Mientras que la Real Academia Española define la informática como:

> *“conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento de la información por medio de computadoras”*.

Estas dos definiciones pudieran parecer un poco vagas, sin embargo son lo suficientemente concretas y claras como punto de partida para desarrollar una definición de “delito informático”. Una primera definición, resultado de fusionar las dos partes, es:

> *“acción u omisión ilícita y culpable en el tratamiento de la información por medio de computadoras expresamente descrita por la ley bajo amenaza de una pena o sanción criminal”.*

La pieza más importante en el ámbito de la computación es la información, y esta primer definición es considerablemente buena porque contempla el manejo de la misma. Algunos de los tratamientos posibles de la información son la creación, edición, eliminación, procesamiento, almacenamiento, transmisión, entre otros. Para realizar el manejo de la información es necesario un sistema de información y una computadora que puede ser una computadora personal, una laptop, un teléfono inteligente, una tableta personal, un servidor entre otros. Aquí se puede

[2] Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. Diccionario jurídico mexicano, Tomo III. México 1983. Pag. 62

identificar un elemento importante en la ecuación, el medio para interactuar con el sistema de información.

Es posible establecer una cadena de interacciones para el manejo de la información, dicha cadena comienza con un usuario, quien utiliza una computadora como medio para interactuar con la información. Sin embargo, internamente la computadora se convierte en un usuario de un sistema de información (el sistema se convierte en medio) que interactúa con una serie de datos para procesar la información. En la figura 1.1 se describen brevemente los sujetos que interactúan en esta cadena de interacciones.

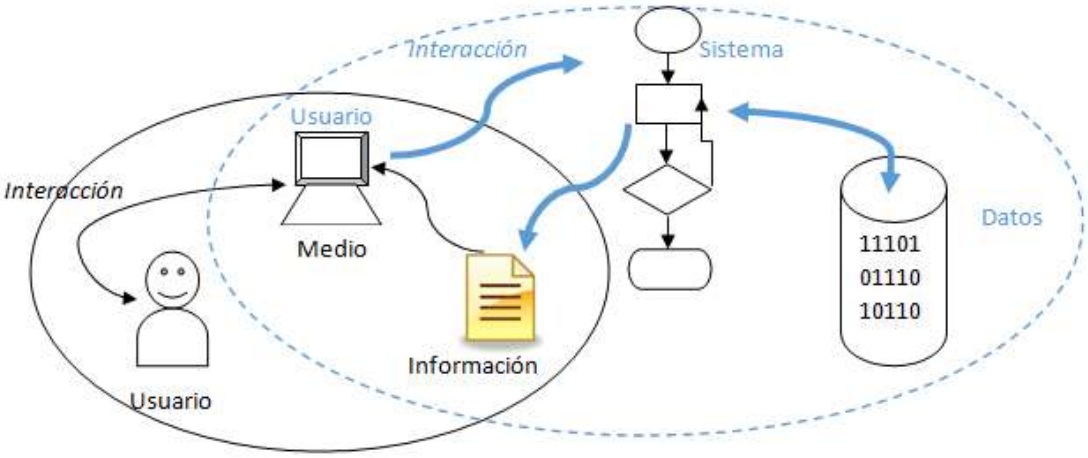


Figura 1.1 Sujetos de la cadena de interacciones

La cadena de interacciones puede ser representada de la siguiente forma: usuario -> computadora -> sistema de información -> datos (ver la figura 1.2).

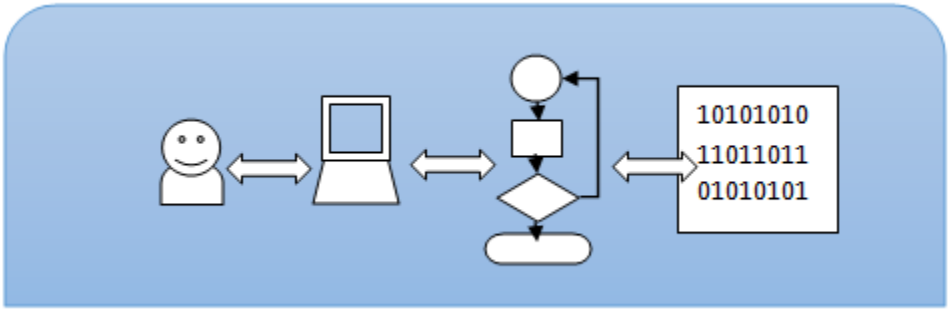


Figura 1.2 Cadena de interacciones

De tal modo que sin llegar a profundizar mucho es posible encontrar otro elemento de la ecuación, los datos. Es importante profundizar hasta este punto porque, en computación, la información es el resultado del procesamiento de una colección de datos individuales. En un nivel más profundo la información es un conjunto delimitado de unos y ceros.

Una vez identificados estos nuevos elementos de la ecuación, la computadora y los sistemas de información como medios y los datos como fin es posible formular una segunda definición de delito informático:

> *Un delito informático es la acción u omisión ilícita y culpable en el tratamiento de datos mediante el uso de un sistema de información a través de una computadora expresamente descrita por la ley bajo amenaza de una pena o sanción criminal.*

De esta nueva definición es posible realizar un nuevo análisis de profundidad, ya que como se mencionó, el tratamiento de datos puede ser a través de una computadora, pero también de varias, es decir, una red. Una red de computadoras se define como un conjunto de dispositivos interconectados entre sí a través de medios de transmisión con el fin de compartir información, recursos o servicios. Una de las redes más importantes que existen es Internet.

Internet se ha convertido en algo más que una gran red de computadoras, hoy en día es parte fundamental de nuestras vidas ya sea de forma directa o indirecta. La importancia que tienen Internet y el uso de las redes en general no pueden pasar

desapercibidas en la definición de delito informático. De tal modo que se puede formular una tercera definición más amplia:

> *Un delito informático es la acción u omisión ilícita y culpable en el tratamiento de datos mediante el uso de un sistema de información a través de una computadora o red de computadoras que se encuentren conectadas o no a Internet, donde dicha acción u omisión se encuentre expresamente descrita por la ley bajo amenaza de una pena o sanción criminal.*

Esta definición expresa conceptualmente la esencia de un delito informático, las palabras *"tratamiento de datos"* abarcan a las acciones antes mencionadas (creación, edición, procesamiento, entre otras) e incluye de manera global a la **triada de la información**, de tal manera que una violación a la integridad de la información está cubierta con el término *"tratamiento de datos"* puesto que en este caso en particular el tratamiento que se le da a los datos sería la edición o eliminación de los mismos, por mencionar algunos. De tal forma que la triada de la información está presente en la definición de manera implícita.

Se puede realizar una comparación entre definiciones, por ejemplo, la definición que ofrece el Consejo Europeo en su *Convenio sobre la* ***Ciberdelincuencia:***

> *"…actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos…"*[3]

En esta definición se incluye de manera explícita a la triada de la información, sin embargo lo que se debe resaltar aquí no son esas tres palabras, confidencialidad, integridad y disponibilidad, sino los activos que pretende proteger, los sistemas informáticos, las redes y los datos. De tal modo que con ese señalamiento se puede mejorar la definición propuesta en este trabajo ya que hasta ahora el único activo que se ha contemplado son los datos, dejando a un lado a los sistemas

[3] Consejo de Europa, Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001. Pág. 2

informáticos y a las redes, y esto es algo que no se puede obviar ya que estos activos también pueden ser víctimas de diferentes tipos de ataque y por lo tanto deben ser contemplados en la definición para protegerlos

Al identificar un nuevo elemento de la ecuación es necesario reformular la propuesta de la definición de delito informático, quedando así:

> *Un delito informático es la acción u omisión ilícita y culpable dirigida en contra de la confidencialidad, integridad o disponibilidad de los sistemas informáticos, redes y/o datos mediante el uso de un sistema de información a través de una computadora o red de computadoras que se encuentren conectadas o no a Internet, donde dicha acción u omisión se encuentre expresamente descrita por la ley bajo amenaza de una pena o sanción criminal.*

Así pues, una vez realizadas varias iteraciones al profundizar y ampliar un poco más la definición, el resultado final es bastante bueno e incluyente. Se ha desarrollado una definición de delito informático partiendo del significado de ambas palabras y haciendo énfasis en lo referente a la informática, añadiendo más términos para conseguir una definición que abarque la mayor cantidad de posibilidades de tal forma que ninguna situación quede fuera del alcance de la definición.

Sin embargo, después de analizar las tres propuestas iniciales y la definición final es posible señalar que la definición de delito propuesta en el diccionario jurídico mexicano se mantiene presente en el producto final prácticamente sin modificaciones. La definición señala claramente que un delito es la acción ilícita expresamente descrita por la ley, por lo tanto no existe margen alguno para tratar de modificar la definición ya que eso implicaría modificar la ley.

Es aquí donde comienza a incrementar la complejidad de este problema. Toda la definición propuesta está sujeta a la ley mexicana y es aplicable solo en los límites de la jurisdicción de este país. Sin embargo, no existen dos países que se rijan por

la misma ley. Por lo tanto la forma en la que un delito informático es descrito en cada país puede variar según las leyes de estos, de ahí el incremento en la complejidad del problema.

Otro elemento involucrado en la complejidad de este asunto es Internet. La importancia y alcance de Internet sobrepasa las capacidades individuales de cualquier país en lo referente a la legislación de delitos informáticos. Cuando este tipo de ilícitos involucran a dos países la computación tiene la capacidad para determinar a los países involucrados y así deslindar responsabilidades, pero el derecho penal de cada país difícilmente está preparado para enfrentar una situación de este tipo.

De tal modo que es muy complicado lograr una definición estándar para los delitos informáticos ya que la situación particular de cada país es diferente de los demás y solo se pueden realizar esfuerzos individuales, como el *Convenio de la Ciberdelincuencia* del Consejo Europeo por ejemplo.

Esta situación de ausencia de estandarización representa una gran ventaja para los delincuentes informáticos o ciber criminales a quienes, en general, no les interesa la nacionalidad de sus víctimas, dentro de la gran variedad de delitos informáticos poco importa que sus objetivos sean mexicanos, chinos o brasileños. Actualmente las acciones que pueden considerarse como un delito informático desde la perspectiva de la computación son muchas y con diferentes objetivos. A continuación se presentan brevemente dichas actividades.

1.2. Tipos de delitos informáticos.

Acceso ilícito a sistemas: Incluye todo tipo de accesos deliberados e ilegítimos a cualquier tipo de sistema informático, ya sea parcial o totalmente al aprovechar algún tipo de **vulnerabilidad** en el mismo con la intención de obtener o alterar de cualquier modo la información contenida o procesada en dicho ambiente, este tipo de delitos también incluye el uso no autorizado del sistema.

Un par de ejemplos de este tipo de ilícitos son los ataques **SQL injection** y los ataques a las redes inalámbricas.

En el primer ejemplo, los ataques vía SQL injection aprovechan una vulnerabilidad en los sistemas basados en web que utilizan el manejador de base de datos SQL para acceder a la base de datos que utiliza dicho sistema sin la necesidad de contar con los datos de autenticación requeridos. De tal forma que el atacante puede llegar a obtener los datos e incluso modificarlos o destruirlos.

En el segundo ejemplo, el ataque a las redes inalámbricas, se aprovecha una vulnerabilidad en el sistema de autenticación, principalmente **WEP,** para obtener la clave de acceso al sistema y así conseguir el servicio de internet. Este delito es uno de los más recurrentes en nuestro país.

Interceptación ilícita de datos: Este tipo de delito se refiere a la interceptación deliberada e ilegítima de datos transferidos a través de una comunicación privada a un sistema de información, ya sea desde un sistema diferente o dentro del mismo sistema. Cualquier tipo de interceptación de datos en una comunicación no pública es un delito informático de este tipo.

Por ejemplo el uso de **keyloggers**, los ataques **Man-in-the-middle** y algunas técnicas para atacar redes inalámbricas caen dentro de esta categoría de delito informático.

Al utilizar un keylogger se está realizando una interceptación deliberada e ilegítima de los datos que son tecleados por el usuario de un equipo de cómputo en donde la comunicación no pública se realiza dentro de un sistema.

Por otra parte, los ataques Man-in-the-middle consisten en hacerle creer a un usuario que se está comunicando con un sistema de confianza cuando en realidad el atacante se está haciendo pasar por ese sistema y actúa como intermediario manipulando la comunicación entre el usuario y un sistema determinado. En este caso la intercepción de datos es más que evidente debido a que el atacante recibe

los datos que el usuario le envía al sistema y una vez que el atacante procesa dicha información la envía a ese sistema de confianza de tal modo que el usuario no se percate de la intercepción.

El tercer y último ejemplo para este tipo de delitos está relacionado con los ataques a las redes inalámbricas. Una manera de conseguir la clave para acceder a la red es interceptar los paquetes que son enviados entre el usuario y el punto de acceso de tal manera que al obtener un volumen elevado de paquetes sea posible encontrar patrones en los datos de cada paquete los cuales representan a la clave de autenticación.

Estos son algunos ejemplos de cómo se puede realizar la intercepción de datos con diferentes métodos.

Interferencia en los datos: este tipo de delitos engloba aquellas acciones que atenten contra la integridad de los datos ya sea que dañen, borren, alteren, deterioren o supriman los mismos. La creación y distribución de **malware** que tenga como fin alguna de estas acciones es un claro ejemplo de este tipo de delitos.

Interferencia en el sistema: la obstaculización deliberada e ilegítima de un sistema informático está clasificada en este tipo de delitos ya sea que esa obstaculización sea por la transmisión, alteración, borrado, deterioro, supresión o introducción de datos.

El ejemplo más claro de este tipo de delitos son los ataques de **negación de servicios**, principalmente distribuidos. Los grupos **hactivistas** como Anonymus utilizan este tipo de ataques para inhabilitar páginas web como forma de protesta. Este tipo de grupos tienen presencia mundial y un gran nivel de miembros y seguidores. Incluso gente que no sabe de computación apoya las acciones y operaciones que estos hactivistas realizan. Los fines que estos grupos persiguen pudieran considerarse loables, sin embargo no sus métodos.

Uno de los métodos utilizados por Anonymus en sus ataques de negación de servicio distribuidos consiste en invitar a la gente a que participe en sus operaciones al acceder a una web que contiene un **script** que realiza cientos de peticiones por minuto a determinada página web, de tal manera que la gente que accede a esos ligas se convierte en cómplice del delito ya que contribuye al ataque de forma automatizada.

Abuso de los dispositivos: este tipo de delitos incluye la producción, venta, distribución y uso de cualquier dispositivo ya sea físico o lógico que sirva como herramienta para realizar algún tipo de delito informático como los antes mencionados y también abarca a la producción, venta, distribución y uso de contraseñas que permitan el uso total o parcial de algún sistema informático. Así como la posesión de dichos recursos (herramientas y/o contraseñas).

Un ejemplo de una herramienta física que puede ser utilizada para cometer un delito informático es un keylogger físico (ver figura 1.3) de tal forma que la producción, venta, distribución, uso y/o posesión de este tipo de dispositivos es un delito informático.

Figura 1.3 Keylogger físico.[4]

[4] http://www.tecnovirus.com/blog/wp-content/uploads/2012/07/Keyloggers.jpg

Una herramienta lógica que cabe en esta clasificación son los programas para obtener contraseñas de redes inalámbricas, antivirus o claves de producto para cualquier tipo de software propietario.

Falsificación informática: este tipo de delitos abarca a las acciones que tengan como fin presentar información falsa de manera deliberada e ilegítima como auténtica con el fin de que dicha información sea tomada en cuenta para efectos legales como si se tratara de información verídica.

El perfecto ejemplo para este tipo de delito informático es el **robo de identidad** en el cual el atacante recolecta la suficiente información de una persona para poder hacerse pasar por ella con el fin de conseguir algún beneficio, principalmente créditos bancarios o para realizar algún fraude.

Fraude informático: son aquellas acciones deliberadas e ilegítimas que tienen como fin obtener algún beneficio económico al alterar la integridad de datos informáticos o al interferir en el funcionamiento de un sistema informático.

El **phising** es un claro ejemplo de este tipo de delitos. En este ataque el objetivo es hacer que la victima proporcione sus datos por medio de algún tipo de engaño, como la **ingeniería social** o la recreación del portal de una entidad bancaria, y una vez que el atacante obtiene esos datos pueda utilizarlos para realizar algún tipo de fraude.

Delitos relacionados con la pornografía infantil: las acciones que contempla este tipo de delito son la producción de pornografía infantil con el fin de difundirá a través de un sistema de información; la oferta, difusión o transmisión y/o adquisición por medio de un sistema informático y la posesión de este tipo de material en un sistema informático o en un medio de almacenamiento.

Delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines: estos delitos incluyen la reproducción parcial o total sin autorización de una obra protegida, así como la oferta, difusión, transmisión, adquisición y/o posesión de este tipo de material.

Esta lista de los diferentes tipos de delitos informáticos está basada en el *Convenio sobre la Ciberdelincuencia*[5] y es una de las más completas que se encuentren disponibles. Sin embargo no contempla los delitos relacionados con amenazas, hostigamiento y acoso en internet. Este tipo de delitos abarcan a las acciones que atentan con la tranquilidad de una persona al utilizar datos informáticos para causar daño psicológico. Un triste ejemplo de este tipo de delitos es el **ciberbulling**, en donde se utilizan redes sociales como medio para amenazar, amedrentar, difamar o hacer burla a una persona.

Estos delitos relacionados con las amenazas, el hostigamiento y el acoso se han acrecentado por el uso de las redes sociales como facebook o twitter por mencionar algún ejemplo. De acuerdo con el estudio sobre los hábitos de los usuarios de Internet en México nueve de cada diez personas accede a alguna red social lo que significa que un gran número de personas se encuentra expuesto a este tipo de delitos, de ahí la importancia de tomarlos en cuenta para que este tipo de actividades sean tipificadas.

Una vez que las diferentes acciones u omisiones que pueden considerarse como delitos informáticos han sido recopiladas es preciso recordar que la definición de delito informático varía para cada país debido a su propia legislación, por lo tanto el conocer la situación de este tipo de delitos de acuerdo a las leyes de México es de suma importancia.

1.3. Los delitos informáticos en la legislación mexicana.

Hasta este momento, año 2014, México no cuenta con una Ley Federal de Delitos Informáticos, sin embargo, existen algunos esfuerzos individuales que pretenden legislar este tipo de ilícitos. Estos esfuerzos son se encuentran en el Código Penal

[5] Consejo de Europa, Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001. Pags 4-8

y en la Ley Federal De Protección De Datos Personales En Posesión De Los Particulares (LFPDPPP).

Dentro del Código Penal Federal, en el título noveno, existe un apartado que lleva por título *"revelación de secretos y acceso ilícito a sistemas y equipos de informática"* el capítulo uno de dicho apartado está dedicado a la revelación de secretos.

Dentro de este primer capítulo se encuentran tres artículos que en pocas palabras expresan lo siguiente:

> ***Artículo 210***.- *"...al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto."*

> ***Artículo 211***.- *"…cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial."*

> ***Artículo 211 Bis***.- *"A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada…"*

En estos artículos se tipifica la revelación de información que puede ser considerada como sensitiva para una persona u organización, en donde las penas varían entre jornadas de trabajo a favor de la comunidad, de uno a cinco años de multa y la suspensión de profesión hasta sanciones entre seis y doce años de prisión y trescientos días de multa respectivamente para cada artículo.

En el capítulo dos, referente al *acceso ilícito a sistemas y equipos de informática* se establecen las acciones, los activos informáticos afectados, los infractores y las sanciones correspondientes contempladas en este tipo de delitos.

A continuación se cita textualmente el artículo 211 bis:

> *"**Artículo 211 bis 1**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa."*

Los demás artículos son similares pero abarcan diferentes acciones, activos e infractores. Es posible resumir la información contenida en esos artículos, del 211 bis 1 al 211 bis 7, y concentrarla en la tabla 1.1 para comprender el tipo de delitos que se tienen contemplados en este capítulo.

Tabla 1.1 Resumen del contenido de los artículos 211 bis 1 - bis 7.

Acción	**Activo Informático**	**Infractor**
Modificar, destruir, provocar la pérdida de información, conocer, copiar.	Equipo de informática protegido por algún mecanismo de seguridad	Cualquier persona
Modificar, destruir, provocar la pérdida de información, conocer, copiar.	Información almacenada en equipos del estado	Cualquier persona. Personal autorizado.

Conocer, obtener, copiar, utilizar.	Información almacenada en equipos de seguridad pública.	Cualquier persona. Personal autorizado. Servidor o ex servidor público.
Modificar, destruir, provocar la pérdida de información.	Información almacenada en equipos del sistema financiero.	Cualquier persona. Personal autorizado.
Copiar.	Información almacenada en equipos del sistema financiero.	Personal autorizado.

Esos son los capítulos correspondientes a delitos informáticos que se encuentran explícitamente en el código penal federal. Sin embargo, también existen menciones de otros delitos informáticos en otros títulos de código. Por ejemplo, en el título octavo, referente a los delitos contra el libre desarrollo de la personalidad, en el capítulo segundo se tipifican las acciones relacionadas a la pornografía infantil.

En los artículos 202 y 202 bis se tipifica la generación, exhibición, transmisión, reproducción, almacenamiento, distribución, venta, compra, arrendamiento, exposición, publicitación, importación o exportación de este tipo de material pornográfico infantil. También especifica qué medios son utilizados como medios para los fines mencionados, dichos medios son redes de datos, sistemas de información, dispositivos de almacenamiento, sistemas de telecomunicaciones, sistemas de audio y video, ópticos y de imprenta, entre otros.

Otros delitos informáticos que se encuentran en el código penal de manera implícita son los contemplados en el título quinto, referente a los delitos en materia de vías de comunicación y correspondencia. En el capítulo primero, *ataques a las vías de comunicación y violación de correspondencia* se encuentran los artículos 167 sección VI y 168 bis.

El artículo 167 tipifica la interrupción o interferencia de las comunicaciones alámbricas, inalámbricas o de fibra óptica por las cuales se transmitan datos. El artículo 168 bis tipifica la decodificación de señales de telecomunicaciones distintas a las de satélite y la posesión de dispositivos que permitan decodificar dichas señales.

Para terminar con los delitos informáticos contemplados con el código penal federal, el título vigésimo sexto, referente a los delitos en materia de derechos de autor menciona en el artículo 424 bis las sanciones para aquellos que produzcan, reproduzcan, introduzcan, transporten, almacenen, distribuyan, vendan o arrienden obras, fotogramas, videogramas o libros protegidos por la L*ey Federal de Derechos de Autor*, así mismo señala las sanción correspondiente para quien fabrique un dispositivo o sistema de información cuya finalidad sea la de desactivar los dispositivos electrónicos de protección de un programa de computación.

Un artículo más, relativo a los derechos de autor es el 426, en este artículo se mencionan las sanciones para quien venda, fabrique, importe o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, así mismo, las acciones que tengan como objetivo dicha tarea también están sancionadas.

Estos son los artículos que ofrece el Código Penal Federal para tratar este tipo de acciones u omisiones relacionadas de alguna forma con un sistema de información.

La LFPDPPP también contempla acciones u omisiones relacionadas al manejo de información personal que pueden ser considerados delitos informáticos de acuerdo a la definición aquí presentada. Esta ley, publicada el 5 de julio de 2010 en el Diario Oficial de la Federación, tiene como objetivo regular el tratamiento de los datos personales en posesión de particulares para garantizar la privacidad de los mismos, además de conceder derechos a las personas físicas que les permiten tener control de sus datos personales en posesión de personas físicas o morales de carácter privado.

La Ley define como dato personal a *"cualquier información concerniente a una persona física identificada o identificable"*[6]. También contempla datos personales sensibles, que son *"aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual"*[7].

El uso que un particular hará con los datos que recabe de sus clientes debe estar explícitamente indicado en un **Aviso de Privacidad**, este aviso debe contar con al menos seis puntos definidos en el artículo 16 de esta ley federal, entre los que se incluyen: la identidad y domicilio de la entidad que recaba los datos, la finalidad que se le dará a los datos recabados, los medios para ejercer los derechos de acceso, rectificación, cancelación y oposición, también conocidos como **derechos ARCO**, entre otros.

Estos derechos son parte fundamental de la ley, ya que permiten que los dueños de los datos personales tengan herramientas para controlar los mismos, por ley, los particulares en posesión de datos personales están obligados ofrecer los medios y mecanismos para que las personas puedan ejercer estos derechos, así como atender las solicitudes de acceso, rectificación, oposición y cancelación de datos personales que sean presentadas en cualquier momento.

Para cumplir con esta obligación, la ley establece que una persona o departamento debe ser asignada como responsable que atienda las solicitudes de los titulares de los datos y así puedan ejercer sus derechos. Estos encargados de

[6] Artículo 3 de la LFPDPPP fracción V.

[7] Artículo 3 de la LFPDPPP fracción VI.

los datos también tienen la responsabilidad de fomentar la protección de los datos personales al interior de la organización[8].

El Capítulo X de la LFPDPPP establece las infracciones y sanciones correspondientes por la omisión o incumplimiento de los artículos contemplado en la ley. Entre las infracciones se encuentra el incumplimiento de solicitudes para ejercer los derechos ARCO realizadas por el titular de los datos, omitir en el aviso de privacidad alguno o todos los puntos definidos en el artículo 16 de la ley, recabar datos de forma fraudulenta o engañosa, entre otros.

Las sanciones contempladas incluyen multas que van de los 100 a 32,000 días de salario mínimo vigente en el Distrito Federal según el tipo de sanción, definidas en el artículo 63 de la LFPDPPP.

La ley, en su Capítulo XI, contempla delitos en materia del tratamiento indebido de datos personales, el artículo 67 establece:

> ***Artículo 67.-*** *Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.*

Este capítulo especifica que las penas establecidas en el mismo se duplicarán cuando se trate de datos personales sensibles.

Con los artículos establecidos tanto en el Código Penal Federal, en la Ley Federal de Derechos de Autor y en la LFPDPPP es posible realizar una clasificación del tipo de acciones u omisiones que se tienen contempladas en la legislación mexicana para realizar un análisis que permita encontrar las áreas de oportunidad relacionadas a los delitos informáticos en esta legislación.

[8] Artículo 30 de la LFPDPPP.

1.3.1. Clasificación de los delitos informáticos en la legislación mexicana.

Es posible agrupar los delitos informáticos contemplados en la legislación mexicana en seis rubros bien definidos según el tipo de actividades involucradas y las repercusiones que estas conllevan:

- Revelación de secretos
- Acceso ilícito a sistemas
- Interferencia en las comunicaciones
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con los derechos de autor
- Incumplimiento de la LFPDPPP

Esta clasificación se basa en los artículos contenidos en el Código Penal Federal, la Ley Federal de Derechos de Autor y la Ley Federal de Protección de Datos Personales en Posesión de Particulares referentes a delitos informáticos y brinda la posibilidad de identificar puntualmente la situación actual de la legislación nacional en esta materia.

Dentro de la clasificación existe el rubro *Revelación de secretos* el cual contempla diversas actividades que pueden atentar contra la confidencialidad de la información, por ejemplo las fugas de información, dicha actividad es bastante común y es realizada diariamente en diferentes ambientes. Cuando una persona se convierte en ex empleado de una organización es muy común que entre las pertenencias que retira de su lugar de trabajo se encuentre un dispositivo de almacenamiento portátil, ya sea una memoria flash o un disco duro. Dicho dispositivo podría contener información sensible para la organización, la cual podría ser usada en perjuicio de la misma por parte del ex empleado. Así como la fuga de información está contemplada en este rubro existen otras actividades que también caben en esta clasificación.

Esta clasificación es complementada con las acciones previstas en el *Acceso ilícito a sistemas*. De tal modo que los accesos no autorizados a diferentes tipos de sistemas informáticos (particulares o gubernamentales) y el manejo que se le da a la información contenida o procesada por dichos sistemas se encuentra contemplada en esta clasificación. Muchas acciones que pueden ser consideradas delitos informáticos caen en esta clasificación. Un claro ejemplo son los ataques *SQL injection* antes mencionados. En estos ataques se pena el acceso no autorizado a la base de datos y la revelación de la información almacenada en ese sistema.

Continuando con la clasificación, la *Interferencia en las comunicaciones* contempla tibiamente los ataques a la disponibilidad de los sistemas y se centra en vías de comunicación en general, por lo tanto hace contemplar diferentes acciones que puedan catalogarse como una interferencia en las comunicaciones, como los ataques de negación de servicio por mencionar alguno.

Los rubros referentes a los *Delitos relacionados con pornografía infantil,* los *Delitos relacionados con los derechos de autor* y el *incumplimiento a la LFPDPPP* abarcan ampliamente las acciones relacionadas con estas actividades y contemplan diversas sanciones para los infractores.

Esta clasificación es el reflejo del estado actual de la legislación mexicana en materia de delitos informáticos, puntualmente hacen falta penas y sanciones para diferentes actividades que pueden considerarse delictivas dentro del código penal federal y por lo tanto hacen falta delitos informáticos por contemplar y clasificar.

Aun existe mucho trabajo por hacer, se ha logrado un buen esfuerzo pero no es suficiente, las actividades delictivas evolucionan más rápido que las leyes de cualquier país que tratan de combatirlas, es por eso que se debe realizar un esfuerzo en conjunto entre expertos en seguridad informática y expertos en derecho para crear mejores condiciones para proteger a las personas y sus vidas virtuales.

Una muestra de las actividades que no están consideradas propiamente en la legislación mexicana y que causan muchas pérdidas económicas para empresas y gobiernos por igual son los ataques de negación de servicio. Estos ataques son una de las principales armas de grupos hactivistas como Anonymus quienes dejan inutilizados sitios web como forma de protesta. Estas acciones no están contempladas como ilícitas dentro de la ley a pesar de las consecuencias que pueden ocasionar.

Es por esto que a continuación se presenta una propuesta para mejorar el código penal federal en materia de delitos informáticos. Es esta propuesta se contempla una gama de actividades que pueden ser consideradas como ilícitas con el fin de ampliar la clasificación de delitos informáticos.

1.3.2. Propuesta de clasificación para la legislación mexicana.

La clasificación actual contempla los siguientes rubros:

- Revelación de secretos
- Acceso ilícito a sistemas
- Interferencia en las comunicaciones
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con los derechos de autor
- Protección de datos personales en posesión de particulares

Sin embargo es posible complementarla con la clasificación propuesta en el *Convenio sobre la Ciberdelincuencia* del Consejo Europeo. Esta clasificación es una de las más completas que existen y es el resultado de la cooperación internacional para combatir este gran problema que afecta a la población mundial con acceso a Internet sin importar su nacionalidad, incluso puede llegar a afectar a las personas que no tienen acceso a Internet.

Debido a la complejidad del problema y su carácter internacional, este convenio es un referente para combatir los delitos informáticos ya que nace por la necesidad de protección para la sociedad amenazada por la ciberdelincuencia y con la idea de la cooperación internacional en mente.

Esta idea, la cooperación internacional, es el punto más sobresaliente de dicha iniciativa del Consejo Europeo, ya que solo trabajando en conjunto será posible hacerle frente a estas amenazas digitales de manera efectiva. Como se ha mencionado anteriormente en este trabajo, la complejidad del problema crece cuando Internet está involucrado y debido al alcance global de esta súper red de comunicación es de suma importancia contar con la cooperación internacional en esta materia, del tal forma que tomar como referencia la clasificación de delitos informáticos ofrecida del convenio sobre ciberdelincuencia para complementar la clasificación según la legislación mexicana resulta apropiado teniendo siempre en mente la cooperación internacional.

Los delitos informáticos son clasificados de la siguiente manera según dicho convenio:

- Acceso ilícito a sistemas
- Interceptación ilícita de datos
- Interferencia en los datos
- Interferencia en el sistema
- Abuso de los dispositivos
- Falsificación informática
- Fraude informático
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines

Es posible encontrar similitudes entre ambas clasificaciones debido a la preocupación que generan ciertos temas a diferentes gobiernos alrededor del mundo. Tanto los delitos relacionados con la pornografía infantil y los relacionados con los derechos de autor son contemplados por ambas instancias debido a la gravedad de dichos comportamientos. Aunque parezca que este par de acciones carezcan del mismo nivel de gravedad es importante señalar que existen ciertos sectores de la sociedad que promueven la criminalización de ciertas actividades cuando estas atentan contra sus intereses.

El claro ejemplo es la protección a los derechos de autor. Las diferentes actividades de piratería atentan contra la riqueza de las industrias del cine, la música, entre otras, de tal modo que esas industrias presionan a los gobiernos para que criminalicen y persigan las actividades de piratería. Y es así como la preocupación por una problemática se convierte en una herramienta para combatir dicho problema, en este caso leyes para combatir la piratería.

Estas acciones son catalogadas como delitos por ambas entidades gubernamentales gracias a la conciencia y preocupación generada alrededor de las mismas. De tal forma que la conciencia de un problema, la identificación del mismo, es uno de los principales motores para comenzar a solucionarlo.

Continuando con la comparación entre estas dos clasificaciones es posible identificar que dentro de la legislación informática son contemplados diferentes delitos dentro de un mismo rubro, el *acceso ilícito a sistemas*. Dentro de esta clasificación se contemplan los accesos no autorizados a cualquier tipo de sistema de información y las posibles modificaciones y manejo a la información contenida en dichos sistemas. En contra parte, el Consejo Europeo propone separar esas actividades para clasificarlas en *acceso ilícito a sistemas, interceptación ilícita de datos* e *interferencia en los datos*.

Esta diferencia en la postura para clasificar las diferentes acciones delictivas no genera ningún conflicto por la discrepancia en la cantidad de rubros clasificatorios ya que dentro del código penal federal estas tres acciones son contempladas

como una sola por la relación e interacción de las mismas, ya que está previsto que ocurra una interceptación o modificación en la información contenida en un sistema informático que ha sido víctima de un acceso no autorizado, y por lo tanto ilícito.

Es en este punto donde se terminan las similitudes entre ambas clasificaciones ya que el rubro referente a la *revelación de secretos* es solo contemplado en la legislación mexicana y los rubros *interferencia en el sistema, abuso de los dispositivos, falsificación informática* y *fraude informático* sólo son contemplados dentro del convenio de ciberdelincuencia.

Esta propuesta para la clasificación de delitos informáticos en la legislación mexicana abarca los rubros recién mencionados ya que cada uno de ellos representa la posibilidad de contar con una herramienta legal para combatir prácticas que afectan a la sociedad de alguna manera.

Algunos ejemplos de dichas prácticas son:

- Revelación de secretos industriales: el rubro de *revelación de secretos* combate este tipo de prácticas en las que empleados de alguna empresa pretendan vender información a empresas competidoras, cuando dicha información es altamente sensible y es manejada por el empleado como parte de sus labores cotidianas.

- Ataques de negación de servicio: la clasificación *interferencia en el sistema* ofrece la posibilidad de ayudar a las empresas que sufren este tipo de ataques por parte de su competencia. De acuerdo al sitio web b:Secure el 50% de las empresas que han sufrido ataques **DDoS** culpa a su competencia de haberlos ejecutado[9].

[9] http://www.bsecure.com.mx/featured/la-mitad-de-las-empresas-acusan-a-su-competencia-de-los-ataques-ddos-recibidos/

- Uso de keyloggers: esta práctica puede ser contrarrestada al incluir la clasificación *abuso de los dispositivos* para proteger a las personas que sufren robo de información mediante este tipo de aparatos.

- Robo de identidad: la clasificación *falsificación informática* es la encargada de contemplar este tipo de acciones que afectan gravemente a la población, tan solo en el estado de Veracruz, México, hasta el mes de agosto del año 2012 los casos robo de identidad se habían incrementado en un 25% respecto al año anterior[10].

- Suplantación de portales bancarios: esta actividad es muy frecuente cuando se pretende obtener información bancaria de una persona para cometer algún fraude, de tal forma que la clasificación *fraude informático* es necesaria.

Estos son solo unos ejemplos de actividades que son realizadas de manera frecuente y que afectan gravemente a la sociedad y gobiernos por igual, del tal manera que es muy importante incluir estos rubros dentro de la clasificación de delitos informáticos si lo que se busca es mejorar las condiciones legales para proteger a cualquier persona de dichas amenazas.

Por último, es necesario incluir un rubro que no es considerado por la legislación mexicana ni por el consejo europeo a pesar de que actualmente se está convirtiendo en una gran problemática en nuestra sociedad. Esta nueva sección es:

- Delitos relacionados con amenazas, hostigamiento y acoso en Internet

Debido al uso que la sociedad le ha dado a las redes sociales y la amplia penetración de las mismas es de suma importancia contar con herramientas para proteger las vidas virtuales de todos y cada uno de los participantes de dichas

[10] http://www.veracruzanos.info/aumento-robo-de-identidad-en-veracruz-25-condusef/

redes. De acuerdo con cifras de la Asociación Mexicana de Internet 9 de cada 10 mexicanos con acceso a Internet es miembro de alguna red social[11] y según un estudio realizado por la compañía Semiocast México se encuentra entre los diez países más tuiteros del mundo con 15 millones de usuarios[12].

Por lo tanto es una gran cantidad de personas que está expuesta a sufrir alguna agresión de este tipo, amenazas, hostigamiento, acoso y es de suma importancia que la legislación mexicana esté preparada para enfrentar estas situaciones.

Una vez que todos estos factores son tomados en cuenta y después de haber realizado un análisis a los elementos disponibles es posible ofrecer una nueva clasificación para los delitos informáticos que pueda ser utilizada como referencia para mejorar las condiciones actuales de la legislación mexicana en esta materia para contar con herramientas que satisfagan las necesidades de protección tanto de la sociedad como de los gobiernos. De tal modo que la clasificación completa es la siguiente:

- Revelación de secretos
- Acceso ilícito a sistemas
- Interferencia en las comunicaciones
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con los derechos de autor
- Interferencia en el sistema
- Abuso de los dispositivos
- Falsificación informática
- Fraude informático
- Delitos relacionados con amenazas, hostigamiento y acoso en internet
- Protección de datos personales en posesión de particulares.

[11] Hábitos de los usuarios en internet en México, AMIPICI. Mayo 2012

[12] http://semiocast.com/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US

Esta clasificación es la suma de dos clasificaciones existentes propuestas por organismos distintos y complementada con un nuevo rubro que surge por la necesidad de combatir un problema creciente y relativamente nuevo, de tal forma que esta clasificación es un reflejo de la actualidad de los delitos informáticos los cuales evolucionan y cambian, crecen según el uso que le den las personas a la tecnología. Lo mismo debe pasar con las herramientas legales para proteger a las personas, deben cambiar y actualizarse para cubrir las necesidades actuales de la gente.

1.4. Elección y justificación de los delitos informáticos a utilizar

A lo largo de este capítulo se ha descrito un panorama actual sobre los delitos informáticos, esta forma de delincuencia es un problema muy grave que afecta a millones de personas alrededor del mundo y poder combatirlo nos es tarea fácil ya que existe un gran número de factores que acentúan la complejidad de esta problemática.

Uno de tales factores es la diversidad de diferentes delitos informáticos que pueden cometerse. Cada día las amenazas informáticas crecen, evolucionan, y se dispersan alrededor del mundo mucho más rápido que las acciones y herramientas disponibles para poder combatir estas amenazas digitales, o al menos para proteger a la sociedad en general de tales amenazas.

Las acciones de protección también son un factor que acentúa la complejidad del problema debido a que las leyes aplicables a este tipo de delitos son la principal herramienta para combatir esta problemática y actualmente no existe un organismo que tenga injerencia a nivel mundial, por lo que cada país debe combatir a los delitos informáticos prácticamente por su cuenta. De tal modo que las legislaciones a nivel nacional deben contemplar este tipo de acciones como delitos y sancionarlas.

El factor relacionado con las legislaciones de cada país debe ser tomado en cuenta antes de contribuir a la lucha contra estos ilícitos, de tal manera que en esta particular contribución los delitos informáticos contemplados dentro del código penal federal son utilizados como base para probar la metodología desarrollada dentro de ambientes controlados. Con la intención de que la herramienta propuesta para combatir la problemática planteada sea de utilidad desde el inicio y no se convierta en una herramienta teórica.

Por lo tanto el primer filtro para la elección de los delitos informáticos es el código penal federal ya que los delitos contemplados en la legislación mexicana podrán ser procesados con mayor facilidad y las probabilidades de sancionar al culpable, en caso de que se pueda deslindar responsabilidades, serán más altas.

Como se estableció en subcapítulo *Los delitos informáticos en la legislación mexicana* los delitos contemplados en el código penal federal son:

- Revelación de secretos
- Acceso ilícito a sistemas
- Interferencia en las comunicaciones
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con los derechos de autor

De este grupo de delitos son los primeros dos, *revelación de secretos* y *acceso ilícito a sistemas,* los que servirán como objeto de estudio dentro de los ambientes controlados con la finalidad de satisfacer uno de los objetivos particulares de este trabajo de investigación, ya que la intención de esta metodología es que pueda ser accesible y utilizada por las pequeñas y medianas empresas que hayan sido víctimas de este tipo de ilícitos.

Según datos extraídos del censo económico 2009 realizado por el Instituto Nacional de Estadística y Geografía (INEGI)[13] el 99.8% de las empresas en México son micro, pequeñas o medianas y en conjunto generan el 52% del

[13] Micro, pequeña, mediana y gran empresa. Estratificación de establecimientos. Censo económico 2009, INEGI

producto interno bruto del país. A pesar de la abundancia de este tipo de empresas existe poca penetración del uso de las Tecnologías de Información (TI) dentro de los procesos de producción de estas empresas y es debido a los altos costos de las soluciones de TI.

Sin embargo, a medida de que los costos de implementar soluciones de TI se vuelven accesibles para las empresas y son incorporadas a los procesos de producción, gestión, administración, entre otros, aparecen los problemas relacionados con la seguridad de la información. Desafortunadamente la implementación de soluciones integrales de seguridad conllevan altos costos para las entidades que adoptan dichas soluciones, por tal motivo pocas veces son puestas en marcha para la protección de los activos informáticos de las empresas. Esta situación vuelve vulnerables a las empresas e incrementa la posibilidad de que estas se conviertan en víctimas de un delito informático.

Es por estos motivos que se ha desarrollado una herramienta accesible para cualquier empresa que permita realizar una investigación completa en caso de haber sido víctima de un delincuente informático con el objetivo de proceder legalmente y deslindar responsabilidades sin que esto implique una gran inversión económica por parte de la empresa afectada.

Por lo tanto, los factores siguientes sirven como parámetro para determinar el tipo de delitos informáticos que son utilizados en los ambientes controlados para probar la metodología desarrollada:

- Delitos informáticos contemplados en la legislación mexicana
- Enfoque de la metodología para el apoyo a las micro, pequeñas y medianas empresas

Una vez seleccionados los delitos utilizados, *acceso ilícito a sistemas* y *revelación de secretos*, los casos de estudio en los ambientes controlados y toda la información referente a este tema se presenta en el capítulo tres con mayor profundidad de detalle.

Capítulo 2

Cómputo Forense

2.1. Introducción al cómputo forense.

El cómputo forense es una ciencia computacional relativamente nueva que surge debido a la necesidad de comprender lo que ha ocurrido en un evento o incidente relacionado con la seguridad de un sistema informático en donde ésta ha sido comprometida por un agente atacante con el objetivo de dañar dicho sistema ya sea destruyendo, modificando o robando información, por mencionar algunas acciones que pueden afectar la integridad, confidencialidad o disponibilidad de un sistema, o conjunto de ellos.

Gracias al cómputo forense es posible determinar las acciones que fueron necesarias para violar la seguridad de un sistema de información y la identidad del culpable de dicha violación, ya sea de manera directa o indirecta. Esta información es el resultado de un análisis exhaustivo a los sistemas vulnerados, en donde gracias a la implementación de técnicas científicas es posible conocer el comportamiento, dentro de dicho sistema, del usuario que perpetro el ataque con la finalidad de conseguir información confiable y contundente para proceder legalmente en contra del atacante para que responda ante la ley por las agresiones realizadas a los sistemas computacionales.

De tal modo que el cómputo forense es a la vez una herramienta altamente especializada de la seguridad informática, ya que requiere altos conocimientos sobre computación, y una herramienta legal que ayuda a la persecución de los delitos informáticos. Esta disciplina técnico-legal tiene como uno de sus objetivos principales el encontrar **evidencia digital** que pueda ser utilizada dentro de un proceso legal como evidencia sólida y contundente para determinar el curso de dicho proceso.

La evidencia digital es el resultado de un **análisis forense**, debe ser concisa y verídica, además de que los métodos utilizados para su obtención deben ser repetibles por cualquier persona, con la finalidad de que su veracidad no sea puesta en duda. Por lo tanto, una de las bases fundamentales de esta disciplina técnico-legal es el método científico.

El método científico proporciona una plataforma bien conocida alrededor del mundo que permite obtener el mismo resultado a cualquier persona que siga paso a paso cada una de las indicaciones que conforman a un experimento. Gracias a la estructura de este método es posible obtener un experimento repetible por cualquier persona que producirá siempre el mismo resultado siempre y cuando se utilicen siempre los mismos datos de entrada y se sigan las instrucciones al pie de la letra.

El método científico consiste en seis etapas:

1. Observación
2. Inducción.
3. Hipótesis.
4. Probar la hipótesis por experimentación.
5. Demostración de la hipótesis.
6. Tesis.

El siguiente diagrama de flujo, que aparece en la figura 2.1, muestra a grandes rasgos la implementación del método científico en una investigación de **cómputo forense:**

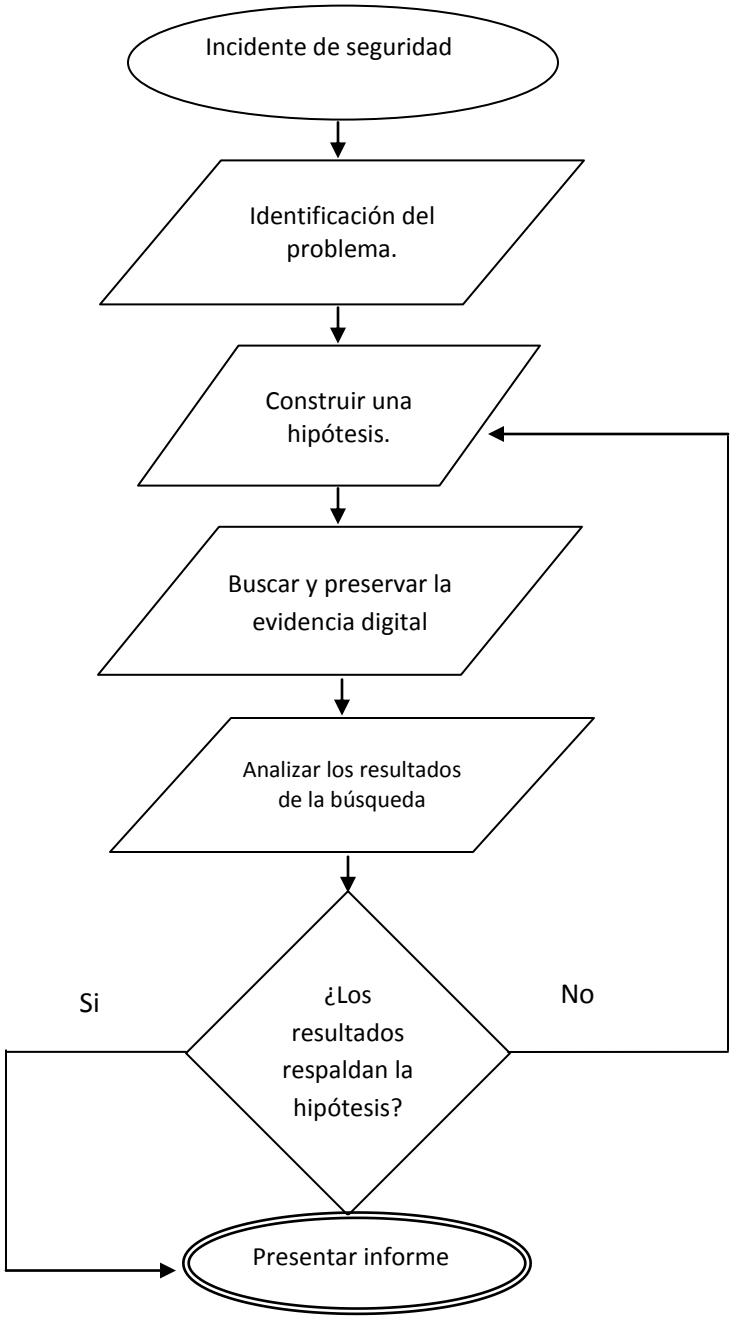


Figura 2.1 Etapas del método científico.

Como se muestra en el diagrama de flujo, toda investigación que utilice el cómputo forense para estudiar un incidente de seguridad comienza precisamente cuando el incidente es detectado. En muchas ocasiones es complicado identificar que la seguridad de un sistema o una red se ha visto comprometida y puede llegar a pasar mucho tiempo antes de que los administradores se den cuenta de la violación. Sin embargo, una vez que se está consciente de que ha ocurrido un incidente de seguridad es preciso identificar el problema.

Dentro del proceso de identificación del problema se encuentran los procesos internos relacionados con la comprobación de la integridad, disponibilidad y confidencialidad de la información contenida en los sistemas y que ha sido víctima de un ataque. Una forma de comprobar la integridad de la información es la comparación de **firmas hash**[14] de los archivos de un respaldo y los archivos que fueron atacados.

De tal modo que una vez identificado el o los activos informáticos que han sido comprometidos es posible formular una primera hipótesis, la cual guiará el curso de la investigación y determinará qué esfuerzos y recursos son necesarios para lograr resultados favorables. Esta hipótesis debe estar compuesta por un plan de acción que delimite puntualmente los alcances de la investigación que deben ser seguidos en todo momento para evitar desperdiciar cualquier tipo de recursos en el proceso de la investigación.

Cuando el plan de acción es puesto en marcha comienza el proceso de análisis donde el primer paso es preservar la integridad de todos y cada uno de los dispositivos involucrados en la violación de seguridad. Dentro de la preservación de los dispositivos existen dos conceptos fundamentales que soportan esta fase del cómputo forense. Estos conceptos son la **cadena de custodia** y las **imágenes forenses**.

[14] En el subcapítulo 2.2 se profundiza en la importancia de las firmas hash.

La cadena de custodia se refiere al proceso de delimitar la interacción de los dispositivos que han sido identificados como dispositivos directamente relacionados con la violación de seguridad que está siendo investigada, es decir, todos aquellos dispositivos que de alguna forma estén relacionados con la pérdida de datos, por mencionar un ataque a la triada de la información, deben ser tratados con extrema precaución y es mandatorio que el acceso a estos dispositivos sea restringido, un control total de estos dispositivos es indispensable para asegurar que la integridad de la información contenida en ellos no sea alterada de ninguna manera, y asimismo garantizar la disponibilidad de ésta para el posterior análisis de resultados, dando como resultado que la confidencialidad de la información se garantiza al implementar este control de acceso.

La correcta aplicación de la cadena de custodia garantizará que la evidencia digital obtenida una vez finalizada la investigación es un reflejo fiel del siniestro ocurrido en el sistema y podrá ser utilizada en el proceso legal como se espera.

El proceso complementario dentro de la preservación de la información es la obtención de las imágenes forenses, estas imágenes son una copia fiel del estado actual del sistema comprometido y son obtenidas a través de la copia de bit a bit y sector a sector del dispositivo físico en donde está alojado el sistema comprometido.

Las imágenes forenses son de gran ayuda en las investigaciones ya que se convierten en el principal objeto de estudio de la investigación, esto es con la intención de preservar intacto el estado actual del dispositivo físico en estudio. La ventaja de las imágenes forenses es que pueden ser replicadas el número de veces que sean necesarias en el transcurso de la investigación, lo cual es de gran ayuda cuando se cometen errores que afectan la integridad del sistema en estudio.

Una vez que el análisis de las imágenes forenses ha concluido y se han encontrado las evidencias digitales buscadas es preciso utilizarlas para validar la hipótesis planteada al inicio de la investigación, de tal forma que respalden y

soporten dicha idea, con lo cual se habrán alcanzado parcialmente los objetivos iniciales. En caso de que la evidencia encontrada, o la falta de la misma no respalden la hipótesis es mandatorio plantear una nueva hipótesis y repetir los pasos que sean necesarios para encontrar la evidencia necesaria.

El último paso de la investigación es la presentación de los resultados obtenidos. En esta presentación se deben incluir dos tipos de reportes, uno es el **reporte ejecutivo**, el cual servirá como la evidencia necesaria para el proceso legal. Este tipo de reporte debe estar redactado en un leguaje sencillo y sin tecnicismos en donde los resultados obtenidos sean mostrados de forma clara y concisa ya que este documento está dirigido a profesionales que no cuentan con una formación especializada en computación.

El segundo tipo de reporte que debe ser redactado es el técnico, en el cual se muestra todo el desarrollo realizado en el transcurso de la investigación. Este reporte sí está dirigido a profesionales de computación y de seguridad informática por lo cual es importante contar con una documentación completa de cada uno de los pasos realizados con énfasis en el porqué se hizo, cómo se hizo y con qué se hizo. Este reporte es igual de importante que el ejecutivo y debe contener información clara, verídica, consistente y correctamente documentada de tal forma que pueda respaldar la investigación en caso de que sea necesario realizar un **contra informe**. Un contra informe es el resultado de una investigación realizada por un investigador forense independiente y sin relación alguna con la primer investigación con la intención de comprobar la veracidad de los resultados obtenidos en la primer investigación.

Actualmente no existe una estandarización para realizar una investigación basada en el cómputo forense, dando como resultado que exista una gran variedad de formas de investigación que tienen sus fundamentos en la experiencia del investigador. Sin embargo, es posible dividir los procesos de una investigación en cuatro etapas bien delimitadas.

Estas etapas son: Identificación, Preservación, Análisis, y Presentación (en la sección 2.3 de este capítulo se profundiza en el estudio de dichas etapas). Esta separación en cuatro fases es resultado del objetivo en común que persigue cada investigador forense, es decir, encontrar la evidencia digital.

2.2. La evidencia digital.

Todas las investigaciones que utilizan el cómputo forense tienen como objetivo último el encontrar evidencia digital, este término representa a todos aquellos registros generados o almacenados en un sistema de información que puedan ser utilizados como evidencia en un proceso legal[15] y que ayude a responder las preguntas planteadas al inicio de la investigación, es decir qué pasó, cómo pasó, qué activos resultaron afectados y quién es el responsable de la violación de la seguridad de un sistema.

Sin embargo para poder lograr la obtención de dicha evidencia es necesario seguir una rigurosa serie de pasos donde la documentación exhaustiva de cada uno de ellos es un proceso fundamental de toda investigación.

Esta serie definida de pasos y consideraciones a tomar en cuenta para cualquier investigación surgen para satisfacer la necesidad de un trato sistemático y documentado de la evidencia digital. Al formar parte de las **ciencias forenses**, el cómputo forense comparte acciones puntuales para el manejo de la evidencia que son utilizadas en la **criminalística**.

[15] Cano, Jeimy. Introducción a la informática forense. Pág. 66

Estas acciones son: identificación, preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección[16].

El manejo correcto de la evidencia digital comienza con la *identificación* de los activos de software o hardware que están involucrados con el incidente de seguridad, una vez identificados comienza el proceso de cadena de custodia para asegurar que dichos activos no se vean comprometidos. La implementación de la cadena de custodia forma parte de la identificación de la evidencia.

En el proceso de la *preservación* de la evidencia es indispensable el uso de **funciones hash**, estas funciones matemáticas convierten una cadena de longitud variable en una cadena de longitud constante. Es decir, la función toma como entrada la información contenida en un archivo y procesa dicha información con una serie de algoritmos matemáticos para generar una firma digital de dicho archivo, donde esta firma es el resultado directo de la información contenida en el archivo original, de tal forma que si dicho archivo es modificado, la firma digital producida por la aplicación de la función hash será diferente.

La implementación de esta función matemática garantiza la integridad de la evidencia digital y respalda los resultados obtenidos al finalizar la investigación. Si se realiza un procedimiento correctamente documentado de obtención de firmas digitales mediante funciones hash se garantiza que los resultados obtenidos al final de la investigación no han sido manipulados en el transcurso de la misma ya que será matemáticamente consistente con la información que se encuentra originalmente en el dispositivo físico.

Una vez que se ha identificado y preservado correctamente la evidencia digital es necesario tomar en cuenta dos factores antes de comenzar con la extracción de información que es utilizada para demostrar la culpabilidad de un atacante. Estos factores son los tipos de evidencia digital que existen y las características específicas de ésta.

[16] Cano, Jeimy. Introducción a la informática forense. Pág. 65

2.2.1. Tipos de evidencia.

Es posible clasificar a la evidencia digital en tres rubros bien definidos según el tipo de activo informático involucrado. Estos rubros son:

1.- Registros almacenados en el equipo de tecnología. Dentro de esta clasificación pueden considerarse los archivos de correo electrónico, los archivos de aplicaciones ofimáticas, las imágenes, entre otros.

La característica de este rubro es que la evidencia digital ha sido manejada y almacenada por el usuario de forma consciente al hacer uso del sistema de información.

2.- Registros generados por el sistema de información. En este rubro se ubican los registros de eventos, registros de transacciones, historial de navegación, entre otro tipo de bitácoras.

La principal característica de este tipo de evidencia digital es que ha sido generada automáticamente por el uso del sistema por parte del usuario.

3.- Registros parcialmente generados y almacenados en los sistemas de información.

En este rubro se encuentran aquellos archivos que son generados al usar el sistema de información y se almacenan en dicho sistema de tal forma que es posible conocer qué usuario ha sido el responsable de haber realizado los últimos cambios en los activos informáticos en cuestión.

Estos tres tipos de evidencia digital son complementarios entre sí y ayudan a ofrecer pruebas contundentes de la culpabilidad de un atacante cuando existe esta evidencia digital.

A manera de ejemplo se presenta el siguiente caso hipotético: una compañía de seguros sufre una fuga de la información de sus clientes, producto de las acciones e iniciativa de un empleado no contento. Una vez realizada la investigación correspondiente es posible identificar al culpable gracias a la evidencia encontrada.

Dentro de los hallazgos de la investigación están los registros de que el usuario correspondiente al empleado inconforme realizó consultas a la base de datos con la información de los clientes (evidencia tipo 3), así mismo se encontró un correo electrónico (evidencia tipo 1) con la información robada dirigido a una cuenta de correo de la competencia de la compañía de seguros, fue posible corroborar que dicho correo fue enviado de la cuenta correspondiente a dicho empelado inconforme.

Y por último fue posible afirmar que ese empleado realizó dichas acciones ya que se encontró el registro de inicio de sesión (evidencia tipo 2) del usuario de dicho empleado de la cual solamente él tiene contraseña.

En este breve ejemplo es posible identificar la interacción de los diferentes tipos de evidencias dando como resultado información veraz, contundente e irrefutable de la culpabilidad de un sujeto, y es gracias al carácter complementario de los tres tipos de evidencias digitales, sin embargo cabe destacar que estos tres tipos de evidencia pueden o no aparecer en el transcurso de la investigación, de tal forma que según la situación y la evidencia encontrada basta con uno, o dos de cualquiera de los tres.

Ya sea que la evidencia digital proporcione información que relacione a un usuario con el delito informático de manera directa, como con el primer tipo, o de manera indirecta (tipo dos y tres de evidencia digital) es necesario tomar en cuenta las

características inherentes de la evidencia digital, ya que estas características guiarán el curso de su recolección.

2.2.2. Características de la evidencia.

Debido a su naturaleza computacional, la evidencia digital posee las siguientes características: es volátil, anónima, duplicable, alterable y modificable, y eliminable.

Dichas características ofrecen ventajas y desventajas en una investigación forense, además dichas características deben ser tomadas en cuenta para guiar el curso de su recolección. El ejemplo más claro de esta situación es la **volatilidad** de la evidencia.

Que la evidencia digital sea volátil implica que ésta debe ser recolectada primero cuando su volatilidad sea más alta, ya que si no es recolectada a tiempo puede perderse sin ser analizada, lo que repercute en los resultados de la investigación. De tal forma que las tablas de direccionamiento (routing) deben ser recolectadas primero, después la información contenida en la memoria RAM y por último los archivos almacenados en discos duros.

Por lo tanto, esta característica se convierte en un parámetro a seguir, y así como la volatilidad de la evidencia establece un parámetro, también la posibilidad de que la evidencia digital sea alterada, modificada o eliminada imponen otro parámetro a tomar en cuenta: la cadena de custodia.

El objetivo de la cadena de custodia es garantizar la integridad de la evidencia, de tal manera que al implementarla se reduce el riesgo de que estas características puedan afectar la información a analizar.

Una de las características de la evidencia digital que proporciona una ventaja para un investigador forense es la duplicidad. Gracias a esta característica de la información es posible realizar múltiples copias idénticas a la original con el objetivo de utilizar dichas copias en la investigación asegurando que la integridad de la evidencia original no sea puesta en riesgo.

Por último se encuentra el anonimato de la evidencia digital. Esta característica representa una desventaja cuando aparece dentro de una investigación forense, ya que implica que la evidencia digital no puede ser vinculada a una persona. A pesar de que es muy complicado que esta característica se presente se debe de tomar en cuenta como una posibilidad existente.

Una vez que se han identificado los tipos de evidencias que existen y se comprenden las características de las mismas es posible comenzar con la investigación forense.

2.3. Principales fases del cómputo forense.

Como se ha mencionado anteriormente, en la actualidad no existe una estandarización que dicte los pasos a seguir para llevar a cabo una investigación utilizando el cómputo forense. A pesar de la falta de estandarización existen varias metodologías de trabajo para realizar una investigación de este tipo.

Entre estas metodologías se encuentran la Metodología Forense del Departamento de Justicia de Estados Unidos, la Metodología Forense del Instituto Nacional de Estándares de Tecnología (NIST), la Metodología de Análisis Forense de la Red Europea de institutos Forenses (ENFSI) y la Metodología de Análisis Forense del Consejo Europeo.

En todas estas metodologías de trabajo es posible identificar similitudes en las acciones que marcan puntualmente para llevar a cabo la investigación. Estas

similitudes pueden ser agrupadas en cuatro grandes fases que son: Identificación, Preservación, Análisis, y Presentación.

2.3.1. Identificación.

La etapa inicial de cualquier investigación forense es la identificación. En esta primera etapa se debe de conocer y documentar perfectamente el estado actual del **sistema vulnerado** y se debe identificar todos y cada uno de los dispositivos que pudieran estar involucrados en el incidente de seguridad, desde computadoras personales, pasando por memorias flash y hasta routers, entre otros. Se debe aplicar la cadena de custodia a cada uno de estos dispositivos con la intención de que el estado actual de estos no se vea alterado, ya que de lo contrario la información necesaria para convertirse en evidencia digital podría llegar a perderse.

Cuando se inicia la cadena de custodia se debe contar con un registro en donde queden asentados los datos de la persona que entrega el bien informático, una descripción de dicho bien en donde se especifiquen cuáles son las funciones del dispositivo y su uso dentro de la red, también debe incluir los datos de los usuarios que lo usan y tienen acceso al mismo, debe incluir la marca, modelo y número de serie del dispositivo. Este primer registro también debe contar con los datos del investigador forense que recibe dicha evidencia, se debe especificar la fecha y hora en la que se realiza la entrega y debe incluir la firma de la persona que entrega el bien informático y de la persona que lo recibe.

También se debe contemplar un control de acceso del bien informático en donde se especifique quién interactúa con dicho bien y porqué, en este documento se deben asentar hora y fecha de la interacción.

Una vez que se ha asegurado el bien informático a través de la cadena de custodia comienza una extensa investigación que tiene como objetivo recopilar

toda la información posible relacionada con dicho bien, o el conjunto de estos, según sea el caso.

Entre la información que se debe recolectar se encuentra aquella relacionada con el entorno legal que protege al dispositivo informático en cuestión para poder trabajar con éste sin que exista alguna traba legal, por ejemplo, es necesario saber si el dispositivo puede ser confiscado para realizar la investigación.

Por lo general se establece un acuerdo con la parte afectada por el delito informático en donde se autoriza por escrito el inicio de la investigación, así mismo se establecen acuerdos de confidencialidad entre la parte afectada y el equipo de investigación forense. En caso de contar con autorización se recomienda no iniciar la investigación.

Otro de los puntos que deben ser investigados son las acciones realizadas en la respuesta al incidente de seguridad, se debe conocer qué se hizo, porqué se hizo, quién lo hizo y cuáles fueron los resultados obtenidos. Esta información debe documentarse y ser avalada por la parte afectada.

Una vez que se conozca lo sucedido en la respuesta a incidentes se debe investigar y documentar el estado actual del sistema, para identificar todas las partes afectadas. Se debe evaluar la gravedad y criticidad de la situación según la sensibilidad de la información afectada, tomando en cuenta la infraestructura de red y los usuarios involucrados. Se debe conocer la topología y el diagrama de la red, obtener los registros de los dispositivos activos dentro de ésta, y también se debe identificar y ubicar el equipo afectado dentro de la red.

Si al realizar la investigación aparece un equipo o dispositivo que esté relacionado con el incidente de seguridad y que aún no se encuentre contemplado dentro de la cadena de custodia es mandatorio que sea registrado y documentado como un bien informático más dentro de la cadena.

Toda esta información bien documentada es la base para realizar la planeación de la investigación, dentro de la planeación es necesario delimitar los alcances de la

misma, así como definir al equipo que debe realizar la investigación y asignar tareas y responsabilidades.

Con toda la información recopilada es posible plantear una primera hipótesis que debe ser tomada en cuenta dentro de la planeación de la investigación. La hipótesis de lo ocurrido debe basarse en los bienes informáticos que se han visto afectados, en los activos informáticos atacados y en las características del sistema y la red de la que forma parte. La intención de esta hipótesis es buscar la evidencia que la respalde y permita finalizar la investigación con los resultados esperados.

La Tabla 2.1 resume los procesos que deben ser realizados en la fase de Identificación:

Tabla 2.1 Procesos a realizar en la fase de identificación.

Acción	Realizado
Aplicación de la cadena de custodia	
Comprobación del entorno legal de los dispositivos	
Autorización de la investigación por escrito	
Acuerdo de confidencialidad	
Documentación de la respuesta a incidentes	
Documentación del estado actual del sistema	
Desarrollo de hipótesis	
Planeación de la investigación	

Una vez que se han completado los procesos correspondientes a esta primera fase se debe proseguir con la Preservación de la información.

2.3.2. Preservación.

En esta segunda fase dentro de una investigación basada en el cómputo forense se encuentran los procesos relacionados con la correcta preservación de la información a investigar. Debido a la naturaleza de estas investigaciones es necesario asegurar que los sistemas de información involucrados en el incidente de seguridad y toda la información almacenada en ellos cuentan con las medidas pertinentes para evitar cualquier tipo de pérdida o modificación de la información.

Para poder comenzar a analizar un sistema es necesario contar con una copia idéntica del mismo y demostrar de manera documentada que la información se mantiene intacta. El primer paso para contar con una copia idéntica del sistema, también llamada imagen forense, es contar con un dispositivo de almacenamiento esterilizado.

Es necesario documentar correctamente el proceso de esterilización para probar que el dispositivo no es causal de alguna modificación que se pudiese presentar en la imagen forense o que el dispositivo no es responsable por la evidencia digital encontrada al final de la investigación, o la falta de la misma. Este proceso de esterilización consiste en eliminar de manera definitiva la información existente, o residuos de la misma en algún medio de almacenamiento.

Una manera de conseguir esto es sobre escribiendo datos en un disco duro, de tal forma que después de repetir el proceso de escritura de datos aleatorios en todos los sectores del disco duro varias veces sea imposible encontrar información en el medio de almacenamiento. Entre más veces se repita el ciclo la posibilidad de encontrar información o residuos de esta en el dispositivo es menor, aunque el costo en tiempo aumenta por cada repetición. Todo el proceso de esterilización debe ser documentado, incluyendo la herramienta utilizada para la realización del mismo, con el fin de demostrar que el funcionamiento de la misma no influye en los resultados obtenidos.

Una vez que se cuenta con un medio esterilizado es posible comenzar con el proceso de creación de la imagen forense del sistema comprometido. Este proceso consiste en copiar toda la información contenía en el sistema comprometido a el dispositivo esterilizado con la finalidad de trabajar con una copia idéntica y reproducible del sistema vulnerado con la seguridad de que la información original no corre riesgo de modificación, voluntaria o involuntaria durante la investigación.

Sin embargo, antes de realizar la copia es necesario considerar la existencia de las áreas **HPA** (Host Protected Area) o **DCO** (Device Configuration Overlay), estas áreas en el disco duro son sectores utilizados por los fabricantes de hardware para almacenar información de configuración de sus productos, en este caso del disco duro. Otro de los parámetros que deben ser considerados antes de realizar la copia idéntica es acceder al medio de almacenamiento digital en modo de solo lectura, para evitar cualquier tipo de modificación en el original durante el proceso de copiado. Existen diferentes herramientas que permiten realizar las imágenes forenses que toman esta consideración de forma automática, lo cual se traduce en menor gasto de recursos en este proceso. Este paso implica documentación de los procedimientos realizados y las herramientas utilizadas.

Una vez que se cuenta con la imagen forense se debe aplicar una función hash a dicha imagen con el fin de contar con evidencia documental del contenido original de la imagen.

El último proceso de la fase de Preservación es el aseguramiento de la imagen forense, este proceso implica un control total del acceso y manejo de la copia original y es de fundamental importancia para garantizar la integridad, disponibilidad y confidencialidad de la información a investigar. Se debe asignar a un responsable de la copia original quien tiene como tarea principal realizar copias idénticas de la primera imagen forense y distribuirlas al equipo de investigación cada vez que estos la soliciten.

Es necesario que se cuente con registros que documenten quién accede a la primera copia original, con qué intenciones y qué acciones realiza con dicha copia y qué herramientas utiliza. Por lo general la única acción permitida es realizar copias idénticas, así mismo se debe registrar quien obtiene dichas copias. Otros datos que forman parte del registro son nombres, fecha, hora y firmas de entrega y recepción.

A manera de resumen, la siguiente Tabla 2.2 condensa los procedimientos fundamentales en la fase de preservación.

Tabla 2.2 Procesos de la fase de preservación.

Proceso	Realizado
Esterilización de medios de almacenamiento	
Identificación de HPA o DCO	
Obtención de imágenes forenses	
Documentación de la salida de la función hash aplicada a la imagen forense	
Generación de copias idénticas de la imagen forense	
Custodia de la primer imagen forense	

Una vez que las imágenes forenses son obtenidas es posible comenzar a analizar la información contenida en ellas. Dicho proceso representa una nueva fase en la investigación, la fase de Análisis.

2.3.3. Análisis.

Cuando el cómputo forense es utilizado en la investigación de un delito informático, o en la investigación de un incidente de seguridad, la fase de Análisis

juega un papel muy importante, debido a su complejidad y los retos que presenta, sin embargo decir que es la fase más importante de la investigación sería irresponsable. Todas las fases tienen la misma importancia, ya que si alguna no es realizada correctamente toda la investigación puede fracasar.

Esta fase se compone de los procesos necesarios para encontrar la evidencia digital que servirá como elemento probatorio legal dentro de un juicio, según corresponda. Estos procesos pueden agruparse en dos categorías: búsqueda y análisis.

Por lo tanto es posible decir que la fase de Análisis se compone de aquellos procesos necesarios para buscar la información contenida en los sistemas de información (archivos de texto, imagen, video, audio, entre otros.) y de los procesos necesarios para analizar la información encontrada. En ciertos casos es posible encontrar información que por sí misma no podría ser considera como prueba de un ilícito pero al correlacionarla con otros elementos de información puede ser posible consolidar dicho conjunto información como evidencia digital robusta y usable.

El primer paso dentro de la fase de Análisis es la verificación de la integridad de la imagen obtenida, cuando la imagen forense es entregada para su análisis se entrega con un documento que entre la información contenida se encuentra el valor del hash de la imagen. La comprobación y documentación de dicho valor es fundamental para iniciar el análisis, debido a que si éste no corresponde con el valor original los resultados obtenidos al analizar la imagen carecen de confiabilidad.

El siguiente paso es identificar cada partición existente en el dispositivo de almacenamiento a investigar, también se debe de tomar en cuenta las particiones anteriores, si es que existe registro de ellas. Así mismo, este análisis da paso a un proceso de búsqueda, si existen varias particiones es posible buscar información que pudiese estar contenida en el espacio entre tales particiones.

Una vez que se han analizado las particiones existentes en la imagen forense es necesario tomar en cuenta la existencia de HPA (Host Protected Area) o DCO (Dymanic Configuration Overlay) para buscar información en dichas áreas del que pudiera estar oculta. La existencia del HPA o del DCO debe ser documentada en la fase de preservación y se debe informar de su existencia en la documentación de entrega de la imagen forense. Es importante tomar estas áreas del disco duro en cuenta ya que los fabricantes las utilizan para almacenar datos de configuración de los dispositivos pero pueden ser usados para ocultar información.

Hasta este punto, toda la información encontrada, según corresponda, en el espacio entre particiones y en el HPA o en DCO debe documentarse para su posterior clasificación, la clasificación de los archivos encontrados se describe más adelante. Todos los archivos encontrados deben ser clasificados.

Continuando con los procesos de esta tercera fase, la fase de Análisis, el siguiente paso a realizar es la identificación del sistema de archivos. Esta identificación del sistema de archivos permite corroborar la información recabada en la fase de Identificación, es decir, si en la fase de identificación se documentó que el equipo vulnerado es una estación de trabajo con sistema operativo Windows, el análisis del sistema de archivos debe permitir confirmar o refutar dicha aseveración.

Una vez identificado el sistema de archivos se procede a identificar el sistema operativo y las aplicaciones instaladas en el sistema. Al identificar estos elementos es posible realizar un análisis de los archivos relacionados con el sistema operativo y las aplicaciones instaladas para descartar aquellos archivos que no han sido modificados y no tienen relación con el incidente de seguridad.

Es posible descartar estos archivos al comparar los valores de funciones hash de los archivos en la imagen forense con los valores de los mismos archivos instalados en un equipo que no ha sido atacado. Esta comparación permite identificar aquellos archivos que no pertenecen a una instalación típica de un sistema operativo o alguna aplicación, donde un instalación típica es aquella que

contiene solo los archivos necesarios del sistema operativo o aplicaciones instaladas por él usuario y donde los archivos no han sido modificados de alguna manera, de tal forma que al comprar es posible encontrar archivos fuera de lugar o archivos modificados y es posible señalarlos como archivos sospechosos.

Estos archivos sospechosos pueden ser el resultado de algún malware, por lo que es necesario realizar una revisión antivirus con software especializado, esto es con el fin de identificar puntualmente aquellos archivos que son residuo del ataque o forman parte del mismo.

Continuando con la fase de Análisis, el siguiente paso es la recuperación de aquellos archivos que han sido borrados, cuando sea posible. Generalmente los archivos eliminados tienen el potencial de convertirse en evidencia digital, ya que los atacantes tratan de borrar sus huellas y el borrado de archivos incriminatorios es básico. Todos los archivos recuperados deben considerarse como sospechosos.

El siguiente proceso a realizar es la búsqueda de información oculta, se deben revisar el espacio fragmentado en el disco duro, los campos reservados en sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos.

El siguiente paso es la recolección de archivos existentes. Todos los archivos que estén almacenados en el sistema deben ser analizados para buscar alguna correlación con el incidente de seguridad. Aquellos archivos que no puedan relacionarse con el ataque son catalogados como archivos sin relación y se documentan. Cuando un archivo almacenado en el sistema se encuentra protegido debe considerarse como potencialmente analizable y se debe tratar de acceder para revisar su contenido. Cuando no es posible acceder a la información protegida, este tipo de archivos se convierten en archivos sospechosos.

Es necesario realizar una clasificación de archivos con el fin de contar con una correcta documentación de los hallazgos encontrados, además de que la clasificación es de gran ayuda cuando se analizan los archivos. Esta clasificación

debe contemplar los rubros para archivos dañinos, sospechosos, inocuos, y potencialmente analizables.

Los archivos dañinos son todos aquellos relacionados con malware conocido, en caso de que el equipo se encuentre infectado, el análisis en busca de virus, y el filtrado de archivos buenos conocidos da como resultado la identificación estos archivos dañinos, que al identificarlos pueden brindar pistas sobre cómo ocurrió la violación de seguridad.

Los archivos sospechosos pueden ser aquellos que tiene una extensión que no corresponde a su contenido, que están en algún directorio que no corresponde al tipo de archivo, los archivos protegidos que no ha sido posible descifrar, diferentes tipos de registro, correos electrónicos, y cualquier archivo que pueda ser relacionado con la violación de seguridad o que pueda tratarse de malware desconocido, entre otros. En esta clasificación se encuentran aquellos archivos que fueron recuperados después de ser eliminados, los ocultos, aquellos alojados en el espacio entre particiones y los almacenados en el HPA o en el DCO.

Los archivos inocuos, o buenos, son aquellos que no tienen relación con el caso o que forman parte del sistema operativo o aplicaciones y no han sido modificados.

Y por último entre los archivos potencialmente analizables se encuentran los archivos protegidos antes de definir si es posible acceder a ellos.

Una vez que se ha recolectado toda esta información es necesario analizarla, buscando patrones de conducta que puedan delatar algún comportamiento anormal en el sistema, o buscar registros de acceso y uso por alguna persona no autorizada, documentos de texto, correos electrónicos, imágenes, registros de llamadas, cualquier archivo que pueda revelar algún dato útil para la investigación.

Realmente es bastante complicado ofrecer un algoritmo para el análisis de los archivos sospechosos, debido a que cada sistema es diferente, y cada violación a la seguridad también lo es. De tal modo que dependiendo del caso a investigar, las circunstancias del sistema, la información y la planeación con que se cuente

esta fase de Análisis varía en cada caso y diferentes algoritmos son utilizados para procesar la información recabada. Una vez terminado el análisis los resultados obtenidos determinan la validez de la hipótesis planteada en la fase de Identificación. Si la hipótesis es validada correctamente el siguiente paso es establecer una línea de tiempo para ubicar los hallazgos encontrados y mostrar su correlación. Si los resultados encontrados no validan la hipótesis es necesario replantear la investigación y comenzar nuevamente.

Cuando los archivos comprometidos encontrados son tantos que sobrepasen la posibilidad de plasmarlos en una línea temporal, los registros documentales de sus hallazgos brindan la validez suficiente para respaldar la evidencia digital encontrada y es posible presentarla en el informe. La correcta documentación de todos los hallazgos es fundamental para conformar un informe ejecutivo y apoyar en el proceso legal.

La Tabla 2.3 muestra los procesos a realizar en la fase de análisis.

Tabla 2.3 Procesos de la fase de análisis.

Proceso	Realizado
Verificación de integridad de la imagen forense	
Identificación de las particiones actuales y anteriores	
Detección de información en los espacios entre particiones	
Detección de un HPA	
Identificación del sistema de archivos	
Determinación del sistema operativo y aplicaciones instaladas	
Filtrado de archivos buenos conocidos	
Revisión antivirus	
Recuperación de archivos borrados Recuperación de información escondida	
Identificación de archivos existentes y archivos protegidos	
Clasificación de archivos	

Consolidación de archivos potencialmente analizables y sospechoso	
Análisis de archivos	
Obtención de archivos comprometidos	
Creación de línea de tiempo	

2.3.4. Presentación.

Esta es la última fase dentro de una investigación de cómputo forense, está conformada por los procesos relacionados con la presentación de la documentación generada en el transcurso de la investigación y la presentación de los resultados obtenidos, así como de una interpretación de dichos resultados. Esta interpretación responde a las preguntas planteadas al inicio de la investigación, de tal modo que dictamina, cuando es posible, quién realizó el ataque al sistema, cómo lo hizo, qué archivos afectó, y cuándo ocurrió el evento. Donde esta interpretación es respaldada por la evidencia digital encontrada y toda la documentación generada.

Cabe destacar que existen varios tipos de informes utilizados para presentar los resultados obtenidos y cada informe está en función del objetivo de la investigación que se realiza. Entre estos informes se encuentran el informe ejecutivo, el **técnico**, el informe pericial, y el contra informe.

El informe ejecutivo tiene como principal objetivo transmitir los resultados de la investigación de forma clara y concisa, omitiendo los detalles técnicos de la investigación y utilizando un lenguaje claro y cotidiano. Este tipo de informe está dirigido a la alta gerencia de las empresas que han solicitado una investigación de este tipo con la intención de conocer el estado de sus sistemas después de un ataque.

Los informes técnicos son aquellos que contienen detalladamente todos los procedimientos realizados durante la investigación, las herramientas usadas y los resultados obtenidos, estos informes están dirigidos a personas altamente capacitadas en cómputo forense.

Los contra informes tienen como objetivo refutar los resultados obtenidos en la primera investigación al realizar una segunda investigación con un equipo diferente y sin relación al primero, es necesario que el informe presente de manera detallada toda la información documental generada durante el proceso de investigación para poder respaldar los resultados obtenidos y así refutar o validar el primer informe.

Por último los informes periciales son aquellos que están dirigidos a un juez y son el resultado de una investigación con el objetivo principal de tomar acciones legales en contra de los responsables del ataque a los sistemas.

Estos informes periciales están constituidos principalmente por tres rubros, el primero de ellos está relacionado con la descripción del estado de la persona u objeto en estudio, esta descripción debe ser realizada por el perito o experto quien realiza la investigación.

La segunda parte del informe pericial contiene una explicación detallada de las diferentes operaciones relacionadas para obtener el informe y del método científico que se ha empleado en la investigación, así como los resultados obtenidos.

La tercer y última parte del informe pericial contiene las conclusiones de la investigación por parte del perito o experto y sus observaciones generales.

Una vez que el informe está terminado el investigador debe presentarlo ante el juez para su ratificación, y de ser necesario, el investigador debe aclarar cualquier término al juez.

La Tabla 2.4 muestra los diferentes tipos de informes, a quien van dirigidos y su objetivo principal.

Tabla 2.4 Tipos de informes.

Informe	Dirigido a	Objetivo	Lenguaje
Ejecutivo	Alta Gerencia	Mostrar el estado del sistema después de un incidente de seguridad para evaluar daños.	Cotidiano, simplificado. Sin tecnicismos.
Técnico	Expertos en cómputo forense	Detallar los procesos realizados y los resultados obtenidos.	Técnico
Contra informe	Alta Gerencia	Corroborar o desmentir los resultados de una primera investigación.	Cotidiano, simplificado. Sin tecnicismos.
Pericial	Corte	Presentar evidencias en un proceso legal.	Simplificado, con términos legales y algún tecnicismo.

Estas son las fases generales del cómputo forense, la mayoría de las investigaciones toman en cuenta las consideraciones mencionadas anteriormente, y a pesar de que se clasifiquen a todos estos procesos de manera diferente, los pasos generales son los mismos, se persigue el mismo objetivo.

Es posible resaltar que uno de los puntos fundamentales dentro de una investigación de cómputo forense es la correcta documentación de todos los procedimientos y resultados. La importancia de este punto se remarca en la metodología presentada en el siguiente capítulo.

2.4. El cómputo forense como herramienta para la persecución del delito.

Las características del cómputo forense permiten que esta disciplina pueda ser utilizada para perseguir y combatir delitos informáticos. Actualmente, esta herramienta computacional es usada alrededor del mundo para combatir a los cibercriminales que en los últimos años han encontrado en Internet un vasto campo de acción para cometer ilícitos.

Cuando una investigación de este tipo es realizada correctamente, las posibilidades de procesar a estos delincuentes por sus crímenes son bastante altas a pesar de la poca preparación que existe en las legislaciones mundiales para combatir este tipo de ilícitos.

Un ejemplo de esta falta de preparación es la aceptación de evidencia digital como evidencia válida en un proceso legal, sin embargo, cada día este tipo de evidencia alcanza una mayor aceptación en los tribunales como un tipo de evidencia aceptada y la tendencia es que a mediano plazo pueda ser aceptada como válida en cualquier parte del mundo, a pesar de la resistencia al cambio de algunos jueces, por ejemplo.

La situación de los próximos años requerirá de expertos en cómputo forense para proteger tanto a sociedad como gobiernos del cibercrimen que, desafortunadamente, seguirá existiendo, cada vez más fuerte y con mayor alcance global.

Capítulo 3

Metodología para la investigación de delitos informáticos con base en el cómputo forense

Hacer uso de una metodología durante el desarrollo de cualquier actividad genera ventajas. Una de estas ventajas es la estandarización de procesos y procedimientos, la cual permite la revisión de los mismos y facilita la identificación de errores y oportunidades de mejora.

Estos procesos y procedimientos estandarizados permiten el desarrollo de actividades especializadas de una manera ordenada gracias a la serie de pasos definidos a realizar que son contemplados en la metodología.

En este capítulo se presenta una guía estructurada para desarrollar una investigación de incidentes de seguridad de la información que pueden ser considerados como delitos informáticos, basada en los principios del cómputo forense.

En esta guía se contemplan las cuatro principales fases de esta disciplina, Identificación, Preservación, Análisis y Presentación. Así mismo se contempla una fase previa de preparación para la investigación.

En el desarrollo de cada fase se presenta de manera puntual los pasos a ser desarrollados y las herramientas documentales que deben ser tomadas en cuenta para realizar la actividad de investigación de manera adecuada.

3.1. Generalidades de la metodología.

Una metodología es un conjunto de métodos que son implementados con el fin de realizar una investigación científica[17]. Estos métodos son aquellos procedimientos que de manera objetiva y precisa son capaces de producir resultados repetibles y verificables en una investigación al ejecutarlos de manera sistemática, esta manera de llevar a cabo un estudio da como resultado una metodología de investigación.

[17] Definición de la Real Academia Española. http://lema.rae.es/drae/?val=metodolog%C3%ADa

Las metodologías de investigación son herramientas que facilitan el estudio de diversos problemas, que pertenecen a una misma área, gracias a que es posible seguir una guía para realizar dicha investigación, donde la guía es independiente al problema, de tal modo que sin importar que los problemas a estudiar sean diferentes, la guía para su estudio es la misma.

Esta característica es una ventaja cuando se pretende investigar delitos informáticos, ventaja que se traduce en una reducción en el tiempo de la investigación ya que la metodología a utilizar es la misma para cada delito que se presente y se requiera estudiar.

Otra de las ventajas del uso de una metodología es que permite una fácil identificación del objeto de estudio, así como del propósito del estudio, el sujeto a quien va dirigido el estudio, el sujeto que realiza el estudio y los alcances del mismo. Toda esta ayuda se traduce en una reducción de tiempos y en una agilización de los procesos relacionados con la preparación necesaria antes de iniciar la investigación.

Una ventaja más que se obtiene al implementar una metodología de investigación es la reducción de recursos invertidos en la análisis de un problema ya que la metodología señala las pautas a seguir de una manera clara y precisa, lo que se traduce en un menor tiempo al investigar un caso.

De tal modo que lo que se busca alcanzar con la implementación de este tipo de herramientas es aumentar la eficiencia de los resultados obtenidos en el estudio de diferentes objetos, facilitar la investigación de los mismos y contar con un registro de todo lo que se realiza durante el estudio de un caso.

Debido a que existe una gran variedad de casos que pueden ser investigados con ayuda de una metodología basada en el cómputo forense es necesario acotar el universo de los mismos con la intención de ofrecer una solución efectiva que pueda ser implementada sin la necesidad de realizar grandes modificaciones en el estudio de delitos informáticos que atenten contra la información de los sistemas que cumplan con el perfil que se desarrolla en el siguiente subtema.

3.2. Una metodología para redes LAN.

Gracias a las redes de datos es posible compartir información y hacer uso de múltiples tipos de servicios que son proveídos por diferentes máquinas que pueden estar en una misma habitación o al otro lado del mundo. Estos grandes sistemas de cómputo que facilitan la vida al permitir este intercambio de información también acentúan la dificultad de realizar investigaciones basadas en cómputo forense.

Es muy distinto realizar una investigación de este tipo a un incidente ocurrido en una red con un par de estaciones de trabajo a investigar un incidente ocurrido en la red de un campus universitario. Entre mayor sea el número de subredes y equipos involucrados en un incidente de seguridad informática mayor es el nivel de complejidad de la investigación y mayor es la capacitación y experiencia que debe tener un investigador para realizar dicho análisis.

Es debido a esta consideración que la metodología aquí propuesta está optimizada para la investigación de incidentes ocurridos en sistemas que cumplan con el siguiente perfil:

> *"redes de propiedad privada que se encuentran en un sólo edificio o en un campus de pocos kilómetros de longitud. Utilizadas para conectar computadoras personales y estaciones de trabajo"*[18]

Es decir, redes de área local (LAN por sus siglas en inglés). La idea detrás de trabajar con este tipo de redes de datos es que este proyecto sirva de apoyo en las investigaciones dedicadas a identificar al infractor de los delitos informáticos en las pequeñas y medianas empresas.

De tal modo que esta metodología puede ser utilizada por personal con un nivel bajo de especialización en cómputo forense, como puede ser un administrador de

[18] Redes de Computadoras, Andrew S. Tanenbaum. Pág. 16

red, un desarrollador de software, o incluso un estudiante de ingeniería en computación (o carreras afines) que curse los últimos semestres. Sin embargo es preciso mencionar que los perfiles mencionados pueden llegar a obtener resultados parciales o incompletos debido a su falta de experiencia, ya que esta característica es un factor importante que ayuda en este tipo de investigaciones.

Asimismo es pertinente mencionar que el material aquí desarrollado le permite a este tipo de personas iniciarse en el campo del cómputo forense ya que brinda una guía de fácil acercamiento que al paso del tiempo y el uso constante de la metodología les permitirá adquirir la experiencia necesaria para obtener cada vez mejores resultados.

Así, la experiencia del investigador es fundamental para llevar a buen puerto una investigación, cualidad que puede traducirse en una menor cantidad de recursos invertidos en la investigación, una mejor interpretación de los resultados e incluso la obtención de resultados concluyentes.

Esta herramienta por sí misma no resuelve investigaciones, ofrece una guía para el desarrollo de las mismas. Aunado a dicha guía se ofrece la posibilidad de contar con materia prima que un investigador experimentado podría convertir en evidencia digital e incluso resultados contundentes. Esta materia prima son las imágenes forenses.

Esta metodología hace un gran énfasis en la obtención de las imágenes forenses, de tal modo que si es seguida al pie de la letra es altamente probable que la imagen obtenida sea igual de útil para obtener resultados contundentes sin importar el grado de experiencia del investigador.

De tal modo que si una empresa decide realizar la investigación por su cuenta y no obtiene resultados satisfactorios con su equipo de investigación, puede solicitar los servicios de un equipo profesional de investigadores forenses quienes no tienen que partir de cero para realizar la investigación ya que previamente se obtuvieron las imágenes forenses y se espera que el proceso de adquisición de las imágenes se encuentre bien documentado.

Cabe señalar que de la misma manera en que esta metodología puede ser utilizada en casos como los ya mencionados, con ciertas modificaciones, puede servir también para investigar otro tipo de incidentes que involucren redes de computadoras más grandes u otros sistemas que no compartan el perfil antes descrito. Las adecuaciones necesarias estarán en función de las características del sistema a investigar y es deber del investigador ajustar la herramienta para que pueda ser aprovechada en tales entornos.

3.3. Metodología propuesta.

La metodología para la investigación de delitos informáticos aquí presentada contempla un escenario donde la seguridad informática de un sistema conectado a una red LAN ha sido vulnerada y dicha violación representa una problemática considerable para la empresa ya que información sensitiva ha sido afectada. Esta exposición de la información requiere de una investigación para que los responsables enfrenten consecuencias legales.

La metodología presenta una serie de pasos a seguir para investigar el incidente de seguridad. Estos pasos recorren las principales fases de una investigación basada en cómputo forense y contempla los siguientes roles para las personas involucradas en todo el proceso de investigación:

- Responsable de la empresa: persona quien solicita la investigación basada en cómputo forense y es quien tiene la autoridad para conceder autorización para que inicie la investigación, así mismo es la persona a quien se le entregan los resultados de la investigación.
- Líder de la investigación: principal investigador y primer responsable del manejo de la información de la empresa.
- Investigador: miembro del equipo de investigación.

- Custodio de la información: persona encargada de garantizar la confidencialidad, integridad y disponibilidad de la cadena de custodia de todos los activos que estén relacionados con la investigación.

Las actividades que realiza cada uno de estos roles son detalladas a lo largo de la metodología en cada uno de los procesos existentes: preparación, identificación, preservación, análisis y presentación.

La metodología está formada por una serie de recomendaciones y ofrece un conjunto de formatos que auxilian en el proceso documental en todas las fases de la investigación, además de que ofrecen una guía para tomar en cuenta diferentes datos en cada proceso.

A continuación se presenta la metodología dividida en los cinco procesos antes mencionados.

3.3.1. Proceso de preparación.

Este proceso tiene como propósito preparar un ambiente adecuado para llevar a cabo una investigación en cómputo forense de manera adecuada, este ambiente debe seguir ciertas consideraciones para garantizar que sus características no intervienen con el curso de la investigación ni con los resultados que se obtienen al manejar la evidencia digital.

Este ambiente adecuado para la investigación en cómputo forense está formado por dos elementos. El primer elemento es la creación de una estación de trabajo con todas las herramientas forenses que pueden ser utilizadas para realizar la investigación. El segundo elemento consiste en documentar el proceso esterilización de las unidades de almacenamiento a ser utilizadas para almacenar las imágenes forenses.

Estación de trabajo.

Para la creación de una estación de trabajo se debe tomar en cuenta las siguientes recomendaciones:

- La elección del sistema operativo debe estar en función de las herramientas especializadas a utilizar.
- El sistema operativo y todas las aplicaciones deben contar con las últimas actualizaciones y parches de seguridad.
- El equipo debe tener un antivirus actualizado, firewall, además de las herramientas de seguridad que se consideren necesarias para garantizar la integridad de la evidencia analizada.
- Contar con respaldo documental de las aplicaciones instaladas utilizadas en la investigación.

Para apoyar el respaldo documental de las aplicaciones es posible aplicar el formato PREIN-APP-01 (Véase la tabla 3.1).

Tabla 3.1 Formato PREIN-APP-01.

Formato PREIN-APP-01 Contiene información sobre las aplicaciones utilizadas en la investigación.	
Nombre de la aplicación	
Desarrollador	
Versión	
Hash MD5 del instalador	
Hash MD5 del ejecutable	
Fuente de descarga	
Fecha de instalación	

Contar con esta información es de utilidad cuando se requiere respaldar el uso de aplicaciones legítimas utilizadas en una investigación.

El siguiente elemento de la fase de preparación es la esterilización de las unidades de almacenamiento destinadas a alojar las imágenes forenses, archivos de volcado de memoria, entre otros, de los sistemas a investigar.

Pala la documentación de este proceso se ofrece un formato (véase la tabla 3.2) diseñado para recopilar la información necesaria para cada dispositivo a utilizar.

Tabla 3.2 Formato: PREIN-EDA-01.

Formato: PREIN-EDA-01 Este formato contiene información relacionada con el dispositivo de almacenamiento esterilizado, técnica de borrado y md5 de la unidad.	
Información del dispositivo	
Marca/modelo	
Número de serie	
Capacidad	
Descripción	
Información sobre la esterilización	
Aplicación utilizada	
MD5 de la aplicación	
Algoritmo utilizado	
Número de pasadas	
Fecha y hora de la esterilización	
Responsable de la esterilización	
Firma del responsable	

Existen diferentes aplicaciones en el mercado que permiten hacer este tipo de esterilizaciones, o borrado seguro. Sin importar qué aplicación sea usada es necesario que se recopile la información mencionada en el formato para contar con un respaldo documental.

La importancia de la preparación de una estación de trabajo y esterilizar diferentes dispositivos de almacenamiento radica en estar preparados para iniciar cualquier investigación en cómputo forense y garantizar que los elementos empleados no intervienen en los resultados obtenidos.

Estos elementos, preparación de una estación de trabajo y la esterilización de dispositivos de almacenamiento deben ser realizados por el equipo de

investigadores, y supervisados por el líder de la investigación. Al desarrollar ambos elementos se concluye con el proceso de preparación.

3.3.2 Proceso de identificación.

El proceso de identificación es el primer proceso relacionado directamente con la investigación. Tiene como objetivo ofrecer un panorama lo más claro posible sobre la situación del sistema y los activos informáticos afectados.

El primer paso que debe realizarse es la redacción de una carta donde se exprese la autorización por parte del responsable de la empresa para que el equipo de investigadores pueda iniciar con los procedimientos de recolección de información y análisis de evidencia. Este documento es muy importante y ninguna investigación debería realizarse sin una autorización por escrito de por medio.

La tabla 3.3 muestra un ejemplo de una carta de autorización.

Tabla 3.3 Ejemplo de una carta de autorización.

Carta de Autorización de Inicio de la Investigación
Fecha: (dd) de (mes) de (año) Por medio de la presente se concede autorización expresa por parte del representante de la empresa **(Nombre de la Empresa)**, **(Nombre del responsable)**, al equipo de investigación liderado por, **(Nombre del líder del investigación)**, para iniciar la investigación en cómputo forense con identificador: **(Identificador de la investigación)**. La investigación contempla la revisión de la estación de trabajo **(Marca/modelo)** con número de serie: **(Número de serie).** Con disco duro marca: **(Marca del disco duro)** modelo: **(Modelo del disco duro)** con capacidad de: **(Capacidad de almacenamiento)** y número de serie: **(Número de serie del disco duro).** Así mismo, el representante de la empresa se compromete a apoyar y proveer todas las facilidades necesarias al equipo de investigación para que éste pueda llevar cabo la tarea sin complicaciones.

_____	_____
Firma del representante de la empresa	Firma del líder de la investigación.

Los elementos importantes de la carta de autorización son el nombre y firma del responsable de la empresa y del líder de la investigación, la fecha y el identificador de la investigación. Este último elemento sirve como referencia para agrupar todos los elementos de información generados durante la investigación. El identificador puede estar compuesto por el nombre del caso, la fecha y algún elemento que identifique a la empresa o entidad que este siento investigada.

El identificador de la investigación es único y debe ser usado en todos los formatos utilizados en la investigación, concatenándose al final del nombre de cada formato.

El siguiente punto a desarrollar es la presentación de un documento donde se exprese el compromiso de realizar un manejo adecuado de la información por parte del equipo de investigación. La tabla 3.4 muestra un ejemplo de una carta de confidencialidad que plasma por escrito dicho compromiso (véase la tabla3.4).

Tabla 3.4 Ejemplo de una carta de confidencialidad.

Carta de Confidencialidad.
Fecha: 7 de mayo de 2013
Por medio de la presente, el equipo de investigación liderado por **(Nombre del líder del investigación)** se compromete a respetar la privacidad de la

información, relacionada con la empresa **(Nombre de la Empresa)**, al considerarla como estrictamente confidencial y de uso exclusivo a los procesos relacionados con la investigación en cómputo forense **(Identificador de la investigación)**, por lo cual, el equipo de investigación integrado por **(Nombre del líder del investigación)** se abstendrá a divulgarla, publicarla, distribuirla a terceros, utilizarla en provecho propio, y de conservar copias, respaldos totales o parciales, ya sean electrónicos o físicos, sin la autorización del representante de la empresa.

_____	_____
Nombre y firma del líder de la investigación	Nombre y firma del representante de la empresa

Después de haber presentado y firmado ambas cartas se debe documentar la información del personal que conforma al equipo de investigación. Debido a la necesidad de tener identificada a cada persona que se involucra en la investigación se ofrece el formato IDE-EIF-01 (véase la tabla 3.5).

Tabla 3.5 Formato IDE-EIF-01.

Formato IDE-EIF-01 Formato con la información de los integrantes del equipo asignado a la investigación forense.	
Identificador del investigador	EIF-DRGV-19981101
Nombre	Demian García
Rol en la investigación	Líder de la investigación
Firma	
Identificación con fotografía	

Una vez firmadas las cartas y presentado el equipo de investigación es posible dar inicio a la investigación. El siguiente paso es realizar un perfil sobre el caso a investigar. El formato IDE-INV-01 está diseñado para recopilar información general sobre la investigación (véase la tabla 3.6).

Tabla 3.6 Formato IDE-INV-01.

Formato IDE-INV-01 Información general sobre la investigación.	
Identificador de la investigación	
Tipo de incidente	
Activo afectado	
Fecha de inicio	
Investigador asignado	
Datos generales de la empresa afectada	
Nombre	
Giro	
Dirección	
Director General	
Contacto	
Firma del Director General	
Identificación oficial con fotografía	

El formato IDE-INV-01 proporciona un panorama general de la investigación en curso, el valor del campo “Identificador de la investigación” debe ser el mismo utilizado en las cartas de autorización y confidencialidad.

El siguiente paso a realizar es la recopilación de información relacionada al incidente. Esta información es proporcionada directamente del usuario del sistema afectado a través de una entrevista, las respuestas que proporcione son utilizadas para formular una primera hipótesis y trazar un plan de acción. El formato IDE-ISE-01 (véase la tabla 3.7) está diseñado para recopilar la información de cada empleado relacionado con el incidente, especialmente las personas entrevistadas.

Tabla 3.7 Formato IDE-ISE-01.

Formato IDE-ISE-01 Información de los empleados de la empresa afectada	
Empleado 1	
Nombre	

Puesto	
Descripción de actividades	
Firma	
Identificación con fotografía	
Todas personas mencionadas en este documento al momento de firmarlo aceptan que la información aquí recabada es verídica.	

Las respuestas de la entrevista deben ayudar a establecer una hipótesis que explique qué fue lo que pasó y permita diseñar un plan de acción. Las siguientes preguntas pueden ser utilizadas en la entrevista, es posible añadir o suprimir incisos si se considera necesario.

a) ¿Qué activo informático se vio afectado en el incidente de seguridad?
b) ¿Dónde se encuentra alojado dicho activo (ubicación física del dispositivo)?
c) ¿Quién es el responsable del equipo en el que el activo se encuentra alojado?
d) ¿Quién tiene acceso a tal equipo?
e) ¿El equipo se encuentra conectado a una red?, de ser así ¿Cuál es la información relacionada con la red?
f) ¿Cuál fue la respuesta al incidente?, ¿Quién se encargó de realizarla?, ¿Qué se hizo?
g) Al inicio de la investigación, ¿El equipo se encuentra encendido o apagado?

Las respuestas a estas preguntas pueden ser condensadas en los formatos IDE-AIT-001, IDE-HWD-001, IDE-HWF-01, IDE-RED-01, IDE-RI-01 (véase la tabla 3.8), según corresponda. El uso de cada formato corresponde a la investigación en progreso y no es mandatorio la implementación de todos ellos.

Tabla 3.8 Formatos para activos de información.

Formato IDE-AIT-001 Este formato contiene información relacionada al activo informático que se ha visto afectado (un formato por cada activo)	
Identificador del activo	
Tipo de activo	
Extensión	
Software asociado	
Descripción	

Usuarios con acceso al archivo	
Equipo en el que está ubicado	*(id del dispositivo)*
Responsable del activo	

Formato IDE-HWD-001 Este formato contiene información relacionada al dispositivo involucrado en un incidente de seguridad.	
Tipo de dispositivo	Estación de Trabajo (PC)/(Notebook)
Identificador del dispositivo	
Marca/Modelo	
Características Generales	
Disco Duro asociado al equipo(1)	
Identificador del disco duro	
Marca	
Modelo	
Número de serie	
Capacidad de almacenamiento	
Tipo de Interfaz	
Ubicación del equipo	
Área a la que pertenece	
Empresa/Organización	
Dirección	
Información adicional	
Responsable del equipo	
Nombre del responsable	
Nombre de usuario	
Puesto	
Correo electrónico	
Teléfono	
Descripción de actividades	
Conectividad	
Red a la que se conecta el equipo	
Tipo de conexión	

Formato: IDE-HWF-01 Este formato contiene información relacionada al dispositivo involucrado en un incidente de seguridad.	
Tipo de dispositivo	Memorias flash/Discos duros externos

Identificador del dispositivo	
Marca/Modelo	
Número de serie	
Capacidad de almacenamiento	
Tipo de Interfaz	
Ubicación del equipo	
Área a la que pertenece	
Empresa/Organización	
Dirección	
Información adicional	
Responsable del equipo	
Nombre del responsable	
Puesto	
Correo electrónico	
Teléfono	
Descripción de actividades	

Formato: IDE-RED-01 Este formato contiene información relacionada a la red y su administración	
Tipo de red	LAN
Tipo de conexión	
Topología de red	
Número de equipos conectados	
ISP	
Administrador de la red	
Nombre	
Correo	
Tel	
Comentario	

Formato: IDE-RI-01 Este formato contiene la información relacionada a la respuesta que se le dio al incidente, en caso de que esta exista.	
Datos del encargado de responder al incidente	
Nombre	
Puesto	
Contacto	
Información de la respuesta al incidente	
Descripción de la respuesta	
Procedimientos realizados	

Herramientas utilizadas	
Bitácoras relacionadas	
Comentarios adicionales	

En caso de que se identifiquen diferentes activos en el transcurso de la investigación se debe utilizar un formato por cada activo informático identificado.

Si el equipo a analizar se encuentra encendido al inicio de la investigación se debe comenzar a recolectar evidencia inmediatamente, dejando a un lado el planteamiento de la hipótesis. En el proceso de Preservación se especifica puntualmente el tipo de información que debe buscarse y recolectarse cuando se presente esta situación. Una vez que se complete la recolección de los datos señalados es posible retomar el punto faltante del proceso de Identificación.

El último paso del proceso de Identificación es el planteamiento de una hipótesis. Hasta este punto se ha recopilado mucha información sobre la empresa afectada, el tipo de actividad que realiza, la información que maneja, los empleados que tiene, las actividades que estos empleados realizan, entre otros datos relacionados directa o indirectamente con el incidente de seguridad que debe ser investigado.

La hipótesis debe ser planteada a partir de la información obtenida hasta este momento, es de utilidad cuando no existió una respuesta al incidente y ayuda a planear la investigación. Cabe destacar que hasta este punto no existe interacción directa con los sistemas afectados.

El proceso de identificación termina con el planteamiento de la hipótesis.

3.3.3. Proceso de preservación.

El proceso de preservar la información involucra a las tareas que tienen como objetivo garantizar la integridad, confidencialidad y disponibilidad de la información del sistema que ha sido comprometido. En este proceso se busca reducir al máximo la cantidad de datos que son perdidos al realizar la investigación. Se debe ser muy cuidadoso en este punto ya que de no realizar correctamente este proceso los resultados que se obtienen al finalizar la investigación pueden ser insuficientes por la pérdida de información o inútiles porque no se puede garantizar la integridad del sistema analizado.

La tarea principal en el proceso de preservación es la correcta implementación de la cadena de custodia. Esta tarea implica un control total de los dispositivos involucrados en el incidente, la obtención, preservación y distribución controlada de imágenes forenses o archivos generados al volcar el contenido de la memoria volátil.

El proceso de cadena de custodia comienza con la compilación de diferentes datos relacionados a la investigación (véase la tabla 3.9), en este punto se debe elegir a un miembro del equipo investigador como el custodio asignado, quien debe encargarse de garantizar la integridad, disponibilidad y confidencialidad de todos los dispositivos contemplados en la cadena de custodia.

Tabla 3.9 Formato PRE-CC-01.

Formato: PRE-CC-01 Este formato contiene la información general relacionada con el proceso de la cadena de custodia	
Identificador de la cadena de custodia	
Identificador de la investigación	
Identificador del custodio asignado	
Descripción de los dispositivos custodiados	
Datos del dispositivo	
Identificador del dispositivo	
Bitácora asociada	

Fecha y hora de inserción a la cadena	

Los dispositivos involucrados en el incidente son aquellos que fueron ubicados en el proceso de identificación y se presume están relacionados directa o indirectamente con el incidente. Cada dispositivo debe contar con una bitácora de acceso al mismo (véase la tabla 3.10).

Tabla 3.10 Formato LOG-CC-01.

Bitácora : *LOG-CC-01* correspondiente al dispositivo: *(Identificador del dispositivo)* perteneciente a la Cadena de custodia: *(Identificador de la cadena de custodia)* de la Investigación: *(Identificador de la investigación)*							
Nombre y procedencia del solicitante	Motivo	Traslado	Fecha y hora de inicio	Fecha y hora de término	Firma	Autorizado por	Firma

La bitácora de acceso al dispositivo es de vital importancia para la cadena de custodia, el custodio asignado debe encargarse que todas las personas que interactúen con el dispositivo cumplan con el registro correspondiente después de haber sido autorizados por él mismo para interactuar con el activo custodiado.

Cuando todos los dispositivos involucrados en el incidente han sido contemplados dentro de la cadena de custodia es momento iniciar la preservación de información de los dispositivos involucrados.

Los procedimientos de preservación se definen en función del estado actual del dispositivo, es decir, se debe implementar un procedimiento específico cuando el dispositivo se encuentra encendido y otro cuando el equipo está apagado.

Los dispositivos encendidos alojan mucha información en la memoria RAM, esta información puede ser de gran utilidad en el transcurso de la investigación, por tal motivo debe documentarse y preservarse. Entre la información que se debe documentar se encuentran los procesos en ejecución, las conexiones de red, los

usuarios con una sesión iniciada en el sistema y fotografías de todos los programas que aparecen en el monitor.

Siempre que sea posible, debe realizarse un volcado de memoria RAM, este proceso consiste en generar un archivo con toda la información que se encuentra en memoria. Éste procedimiento solo debe realizarse cuando el equipo sospechoso se encuentre encendido antes de iniciar la investigación. El tratamiento a este archivo es el mismo que el de una imagen forense.

El formato PRE-GVM-01 (véase la tabla 3.11) muestra la información que debe ser documentada en este procedimiento.

Tabla 3.11 Formato PRE-GVM-01.

Formato: PRE-GVM-01 Este formato contiene información referente a la generación del volcado de memoria.	
Identificadores	
Identificador del volcado de memoria	
Identificador del dispositivo origen	
Identificador de la cadena de custodia a la que pertenece el dispositivo	
Identificador del dispositivo donde se aloja el volcado de memoria	
Información de la generación de la imagen	
Herramienta usada	
MD5 de la herramienta	
Identificador del dispositivo donde se aloja la imagen	
Nombre del archivo generado	
MD5 de la imagen generada	
Formato de la imagen	
Tamaño de la imagen	

Responsable de la generación del a imagen	
Firma del responsable	
Hora y fecha de la generación	
Identificado de la bitácora de hashes	

Después de realizar el volcado de memoria RAM o cuando el equipo sospechoso se encuentre apagado se debe generar una imagen forense del dispositivo de almacenamiento. Existen dos vías generales para realizar este proceso, una es por hardware, utilizando una copiadora de discos duros y la otra es por software. Debido al alto costo de las copiadoras de discos duros la metodología se enfoca en el uso de software para realizar las imágenes forenses.

Independientemente de la aplicación utilizada, el procedimiento debe ser documentado con ayuda del formato PRE-GIF-01 (véase la tabla 3.12) y la imagen generada debe ser almacenada en un dispositivo esterilizado. El formato PRE-GIF-01 también puede ser utilizado para documentar un volcado de memoria.

Tabla 3.12 Formato PRE-GIF-01.

Formato: PRE-GIF-01 Este formato contiene información referente a la generación de las imágenes forenses.	
Identificadores	
Identificador de la imagen forense	
Identificador del dispositivo origen	
Identificador de la cadena de custodia a la que pertenece el dispositivo	
Información de la generación de la imagen	
Herramienta usada	
MD5 de la herramienta	
Identificador del dispositivo donde se aloja la imagen	
MD5 de la imagen generada	
Formato de la imagen	
Tamaño de la imagen	
Responsable de la generación del a imagen	

Firma del responsable	
Hora y fecha de la generación	
Identificado de la bitácora de hashes	

Es importante que se generen dos imágenes forenses en dos dispositivos de almacenamiento distinto. Al finalizar su generación, ambas imágenes, usando el mismo formato, deben tener la misma firma digital. Después de generar ambas imágenes, una de ellas debe ser resguardada como respaldo y en caso de necesitar una nueva imagen forense se debe obtener a partir del respaldo. Se debe evitar utilizar el dispositivo original para generar más imágenes forenses.

Una vez que se ha generado la imagen forense se debe obtener una lista de firmas digitales de cada archivo y documentarla según lo establecido en el formato PRE-LHA-01 (véase la tabla 3.13).

Tabla 3.13 Formato PRE-LHA-01.

Formato PRE-LHA-01 Este formato contiene información sobre el listado de hashes de todos los archivos en la imagen forense		
Identificador de la imagen		
MD5 de la imagen		
Lista de firmas		
Archivo	Firma Hash	Fecha

Este listado de firmas se realiza de manera recursiva para todos los archivos que estén almacenados en la imagen forense. El objetivo de este listado es servir como respaldo para asegurar al final de la investigación que los resultados obtenidos no están en conflicto con los archivos originalmente almacenados en el sistema, es decir, que los resultados obtenidos son archivos que se encuentran en el sistema y no han sido alterados.

El custodio de la cadena es el responsable de la recopilar esta información y añadirla a la cadena de custodia. Así mismo, el custodio es el encargado de llevar un control de la generación y distribución de copias de la imagen forense para que

estas acciones cumplan con los lineamientos del manejo adecuado de la información.

Cuando el proceso de cadena de custodia se ha implementado según lo planteado y se han generado las imágenes forenses correspondientes termina el proceso de preservación y se da paso al proceso de análisis.

3.3.4. Proceso de análisis.

El proceso de análisis tiene por objetivo encontrar y preservar elementos de información que puedan ser considerados como evidencia y que sustenten la hipótesis planteada sobre el incidente de seguridad. Debido a que cada investigación es diferente, es difícil ofrecer una serie de pasos específica a seguir para encontrar dichos elementos de información, sin embargo, es posible ofrecer algunas recomendaciones sobre dónde y qué buscar.

Lo primero que debe tomarse en cuenta es si el sistema afectado se encuentra encendido o no. Cuando el sistema se encuentra encendido y en ejecución con una sesión iniciada se debe realizar un análisis en vivo en el cual se debe documentar y recuperar toda la información volátil en el sistema. La información volátil incluye el registro de las aplicaciones abiertas por el usuario, los procesos en ejecución y las conexiones del sistema, entre otros.

Para documentar la actividad actual del sistema y registrar todas las aplicaciones en ejecución, pueden tomarse fotos de la pantalla y de cada aplicación abierta. Para recuperar información sobre procesos y conexiones se recomienda utilizar aplicaciones que no necesiten de instalación para funcionar. Todos los hallazgos deben ser documentados indicando la mayor cantidad de información posible relacionada al proceso o conexión identificada.

Estos hallazgos pueden ser documentados a través de formatos similares al mostrado en la Tabla 3.3.14 donde se asienten los datos más relevantes de la información recopilada.

Durante el análisis en vivo es recomendable realizar un volcado del contenido almacenado en la memoria RAM. Para ello se recomienda utilizar una aplicación que no necesite de instalación y un dispositivo de almacenamiento extraíble, como una memoria flash.

Una vez que se ha realizado el volcado de memoria el sistema debe ser desconectado de la fuente de alimentación para iniciar el análisis forense. Si al llegar al lugar donde se encuentra el equipo a analizar y éste se encuentra apagado por ningún motivo debe ser encendido.

El curso de la investigación está definido por la hipótesis planteada, y la hipótesis se formula con base en la información relacionada con el incidente, por tal motivo, el primer paso en la investigación debe estar encaminado hacia los registros generados por la aplicación relacionada al activo afectado.

Estos registros pueden encontrarse en forma de un historial de navegación, registro de eventos, correos electrónicos almacenados en el equipo, entre otros. Es por esto que se recomienda buscar documentación oficial de la aplicación en cuestión para identificar donde se encuentran alojados estos registros.

También es recomendable realizar búsquedas de cadenas o palabras clave relacionadas con el incidente. Estas palabras pueden ser utilizadas como nombre de archivos, pueden estar registradas en el historial de navegación web o formar parte de algún documento. Cualquiera de estos elementos podría ser evidencia de comportamiento inusual o no autorizado y estar relacionado con el incidente.

Independientemente del enfoque utilizado para identificar la evidencia se debe documentar cada hallazgo relevante. Un hallazgo relevante es aquel que esté relacionado con el incidente de manera directa o indirecta. La información debe

ser compilada en el formato INV-HED-01 (véase la tabla 3.14), el cual debe ser usado por cada hallazgo obtenido.

Tabla 3.14 Formato ANA-HED-01.

Formato ANA-HED-01 Este formato incluye información sobre los hallazgos identificados en la investigación.	
Identificador de la imagen forense	
Identificador del hallazgo	
Nombre del hallazgo (archivo)	
Ubicación del hallazgo (archivo)	
Hash MD5 del hallazgo	
Descripción	
Identificador del dispositivo de almacenamiento usado para copiar el hallazgo	

Cada hallazgo debe ser correctamente documentado ya que estos determinan el resultado de la investigación. Un punto importante a tomar en cuenta es la hora y fecha de modificación o último acceso al archivo, este atributo ayuda a comprender la sucesión de eventos y ofrece un énfasis en la importancia del hallazgo identificado

Cuando la investigación no rinde frutos favorables después de seguir la hipótesis planteada al inicio de la investigación, se recomienda replantear la hipótesis añadiendo los nuevos elementos de información obtenidos hasta el momento. El replanteamiento de la hipótesis solo afecta al proceso de análisis de evidencia presentado en esta metodología.

Durante el desarrollo de una investigación es posible identificar archivos sospechosos que pudieran ser malware relacionado con el incidente investigado, para estos casos se ofrece una guía para un análisis básico de malware.

Este análisis se enfoca en el análisis dinámico de un archivo sospechoso. Para ello se requiere ejecutar dicho archivo en un ambiente controlado con la intención de identificar los cambios que suceden en el equipo una vez que se ejecuta. El análisis de dichos cambios puede arrojar información relacionada con el incidente.

La guía para el análisis básico de malware se compone de cinco pasos:

Paso 1. Creación de un ambiente virtual similar al sistema investigado.

El objetivo es crear un ambiente controlado que cuente con características similares al sistema donde se encontró el archivo sospechoso. Se debe instalar el mismo sistema operativo utilizado en el sistema investigado.

Paso 2. Documentar el estado del sistema recién instalado.

El objetivo de este paso es registrar el estado normal del sistema, particularmente los procesos en ejecución, las conexiones de red y las aplicaciones que se ejecutan al iniciar el sistema.

Paso 3. Infectar el sistema virtual.

En este paso se ejecuta la aplicación sospechosa de ser malware en el ambiente controlado y se observan y documentan los cambios visibles a simple vista.

Paso 4. Documentación del estado del sistema infectado.

Una vez que se ha infectado el equipo se realizan las mismas acciones señaladas en el paso 2, listar los procesos y conexiones red activos así como las aplicaciones que se ejecutan al iniciar el sistema. Cuando se identifican nuevos archivos generados por el malware, estos deben ser extraídos del sistema y se les debe considerar como un hallazgo.

Paso 5. Conclusiones del análisis básico de malware.

Usualmente, el malware realiza modificaciones en el sistema operativo que garantizan su ejecución y ayudan a mantenerlo oculto haciéndolo parecer un archivo del sistema. Cuando estas modificaciones son identificadas al comparar el estado del sistema controlado antes y después de la infección se genera una conclusión que puede ser de utilidad en la investigación realizada.

Estas recomendaciones componen el proceso de análisis perteneciente a la metodología para la investigación de delitos informáticos basada en cómputo forense. El último proceso contemplado en la metodología es el de presentación, que se expone a continuación.

3.3.5. Proceso de presentación.

El proceso de presentación está conformado por dos elementos, el reporte ejecutivo y el reporte técnico. La finalidad de estos dos reportes es presentar los resultados obtenidos al concluir con la investigación en cómputo forense. Cada uno de los reportes está dirigido a dos audiencias diferentes, por lo que su constitución difiere en varios puntos.

El reporte ejecutivo debe ser breve y conciso, no debe exceder una cuartilla y debe estar carente de tecnicismos. Debe presentar un breve resumen del incidente ocurrido en el que se mencione cómo se vio afectada la empresa por el incidente. Este reporte debe contar con los hallazgos identificados explicados de manera clara y concisa y con una conclusión general de la investigación.

En contra parte, el reporte técnico no tiene un límite específico de cuartillas, consiste en un explicación minuciosa de cada paso realizado durante la investigación. En él se deben plasmar todos los detalles posibles sobre las acciones y herramientas utilizadas con el objetivo de que los resultados obtenidos al finalizar la investigación puedan ser replicados por un tercero al seguir los

mismos pasos descritos en el reporte partiendo de la evidencia asegurada en la cadena de custodia, por lo general una imagen forense.

En este reporte se deben incluir todos los formatos utilizados con la información recabada. El lenguaje utilizado en este reporte puede ser totalmente técnico ya que va dirigido a especialistas en la materia encargados de revisar el desarrollo de la investigación para validar o refutar los resultados obtenidos.

El reporte técnico también debe incluir todos los hallazgos identificados, debidamente documentados, en el transcurso de la investigación y que soportan la hipótesis planteada.

Uno de los objetivos de esta metodología es ofrecer herramientas para generar un proceso documental durante el transcurso de cada investigación, por lo que todo el contenido del reporte técnico es generado con forme se avanza en la implementación de la metodología. De tal forma que al final basta con compilar toda la información generada y profundizar con textos explicativos en los pasos que sean necesarios para generar el reporte técnico.

Se recomienda que el reporte técnico contemple los siguientes puntos en su estructura:

- Portada
- Aviso de confidencialidad
- Índice
- Antecedentes
- Actividades realizadas
    - Desglose de actividades
- Conclusión
- Recomendaciones
- Anexos

Uno de los puntos que se destaca es el “Aviso de confidencialidad”, en él se plasma la propiedad de la información contenida en el reporte e indica los límites

de uso de la misma, además de especificar que el equipo de investigación guarda una copia del reporte para incluirla en el expediente de la investigación.

Al igual que los procesos anteriores presentados en esta metodología, el proceso de presentación es susceptible a ajustes o modificaciones según corresponda y se considere conveniente.

En los capítulos 5 y 6 se presenta la implementación de la metodología en la investigación de un delito informático en un ambiente controlado, de tal forma que al finalizar con la investigación se ofrece un ejemplo de ambos reportes, ejecutivo y técnico, para la mejor comprensión de su redacción.

Con la redacción de ambos reportes termina el proceso de presentación, el último proceso de la metodología propuesta en este trabajo de investigación.

Capítulo 4

Ambientes controlados para la implementación de la metodología.

La implementación de la metodología para la investigación de un incidente de seguridad, que puede ser considerado un delito informático, es un punto fundamental dentro de este trabajo de investigación, ya que de esta manera es posible obtener un panorama del desempeño de la metodología en casos prácticos.

La investigación de un incidente de seguridad en un sistema comprometido implica la interacción con información que puede ser confidencial y de carácter sensible para los dueños de la misma, por tal motivo, la aplicación de la metodología se realiza en sistemas dentro de ambientes controlados.

Gracias al uso de este tipo de ambiente es posible poner a prueba, de manera didáctica, la metodología propuesta, garantizando que la información con la que se interactúa es de carácter ilustrativo y su presentación no representa riesgo alguno para un tercero.

A pesar de que el uso de ambientes controlados ofrece cierto grado de flexibilidad para la aplicación de la metodología se ha buscado representar situaciones lo más cercanas a la escena que vive actualmente en el mundo de las MIPYMES y así ofrecer contenidos de consulta actualizados, generados al aplicar la metodología en los escenarios propuestos.

En este capítulo se presenta la importancia de utilizar ambientes controlados, las características que estos deben de cumplir para ser compatibles con los alcances de la metodología propuesta, las descripciones de los escenarios a implementar en los ambientes controlados para los casos A y B y los detalles técnicos de los mismos.

4.1. Uso de ambientes controlados.

El uso de ambientes controlados en el ámbito de la seguridad de la información es bastante recurrente y es considerada una buena práctica para poner a prueba diferentes tipos de conceptos. En estos ambientes controlados las condiciones iniciales de un sistema son bien conocidas y se encuentran documentadas de alguna manera, esto con el fin de que dichas condiciones iniciales no afecten o interfieran en la demostración de algún concepto o en la realización de una prueba.

En los ambientes controlados se simula el funcionamiento de algún sistema que opera en la vida real con el objetivo de realizar pruebas que involucren cierta interacción con el sistema en cuestión. De esta forma, al utilizar un ambiente controlado se puede realizar cualquier tipo de prueba con condiciones similares o iguales al sistema en producción sin afectar el correcto funcionamiento del mismo.

Otra de las razones por las cuales se utiliza este tipo de escenarios recreados es la ética. Ciertas prácticas en la seguridad de la información implican la intervención de los sistemas para alterar su funcionamiento donde algunas veces el resultado de dichas intervenciones es la revelación de información confidencial.

Es por esto que se ha decidido trabajar con ambientes controlados diseñados específicamente para probar la metodología aquí propuesta con el fin de no revelar información confidencial de manera total o parcial en perjuicio de terceros. El estudio del rendimiento de esta metodología en ambientes reales se propone para futuros trabajos donde el interesado debe acordar con los dueños de la información el manejo de la misma durante la realización de dicho trabajo de investigación.

4.2. Características de los escenarios a investigar en ambientes controlados.

Los escenarios a investigar, implementados en ambientes controlados, deben de cumplir con ciertas características para que sean adecuados a las condiciones contempladas por la metodología. La primera condición a satisfacer es que dicho ambiente o escenario virtual refleje el estado de un sistema de cómputo que haya sido víctima de un delito informático. La segunda condición es que el sistema afectado pertenezca al conjunto de sistemas cuyo perfil es contemplado en el diseño de la metodología de investigación presentada en este proyecto.

Para cumplir con estas condiciones se debe contemplar lo siguiente:

1.- De acuerdo a la definición de *delito informático* desarrollada en el capítulo uno se considera que:

> *Un delito informático es la acción u omisión ilícita y culpable dirigida en contra de la confidencialidad, integridad o disponibilidad de los sistemas informáticos, redes y/o datos mediante el uso de un sistema de información a través de una computadora o red de computadoras que se encuentren conectadas o no a Internet, donde dicha acción u omisión se encuentre expresamente descrita por la ley bajo amenaza de una pena o sanción criminal.*

En donde los documentos que compilan las descripciones de las acciones u omisiones que son consideradas como delitos informáticos y sus penas o sanciones correspondientes son el Código Penal Federal, La Ley Federal de Derechos de Autor y la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Siendo así que estos documentos ofrecen el punto de partida para la planeación de un ambiente virtual susceptible a ser víctima de un delito de este tipo.

2.- La metodología de investigación está optimizada para trabajar con sistemas que pertenezcan a la categoría de Redes LAN en donde el perfil de dichos sistemas es el siguiente:

> *"redes de propiedad privada que se encuentran en un sólo edificio o en un campus de pocos kilómetros de longitud. Utilizadas para conectar computadoras personales y estaciones de trabajo"*[19]

Estas dos consideraciones establecen los parámetros de acotamiento para el universo de posibles combinaciones de delitos informáticos y sistemas afectados a simular en un ambiente controlado.

Tomando en cuenta dichos parámetros se define que los delitos informáticos contemplados en el Código Penal Federal son los que se consideran para su desarrollo en los ambientes controlados debido a la variedad de acciones contempladas en este documento. Las acciones penadas en el Código Penal Federal son aquellas que atenten contra la Confidencialidad, Integridad y Disponibilidad de la información de sistemas en equipos protegidos por algún tipo de mecanismo de seguridad, además de los equipos del Estado, equipos de Seguridad Pública y equipos del Sistema Financiero.

El último parámetro a considerar para la definición del universo de delitos y sistemas se toma en cuenta uno de los objetivos particulares del trabajo de investigación, que es desarrollar una metodología que sea accesible para las pequeñas y medianas empresas. Por lo tanto, el universo resultante es el de los equipos protegidos por algún tipo de mecanismo de seguridad pertenecientes a una Red LAN y que estén involucrados en las actividades de una pequeña o mediana empresa.

El Código Penal Federal contempla las siguientes acciones como causales de una pena o sanción cuando son realizadas por cualquier persona en contra de un equipo protegido por algún tipo de mecanismo de seguridad: sin previa

[19] Redes de Computadoras, Andrew S. Tanenbaum. Pág. 16

autorización modificar, destruir, conocer, copiar o provocar la pérdida de información.

Estas acciones se reflejan en los dos tipos de ataques cibernéticos que afectan con mayor frecuencia a las PYMES: el robo de información y el espionaje industrial. De acuerdo al informe anual correspondiente a 2012 desarrollado y publicado por la empresa Symantec "*Informe Sobre Amenazas a la Seguridad en Internet, Volumen 18*"[20] la cantidad de ataques dirigidos se incrementó un 42% respecto al número de ataques de este tipo registrado en 2011. Del total de ataques dirigidos contabilizados por Symantec, el 31% de éstos afectó a empresas formadas por uno o hasta 250 empleados, incrementando un 13% respecto a 2011.La siguiente figura muestra el porcentaje de ataques dirigidos a empresas por su número de empleados.

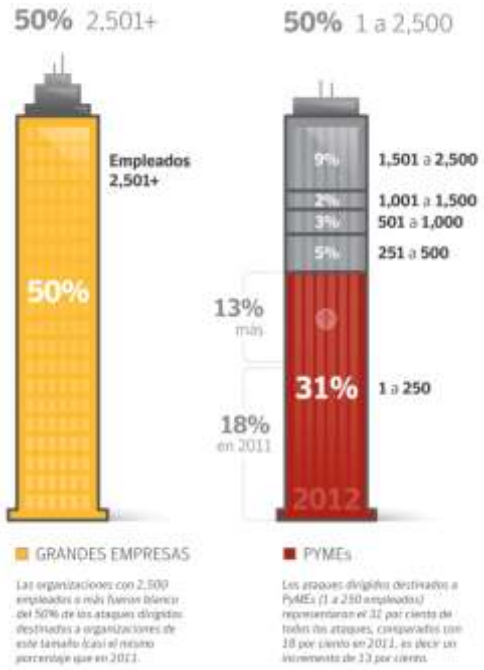


Figura 4.1 Ataques por tamaño de la organización objetivo[21].

El incremento en éste tipo de ataques no es algo sorpresivo si se considera que existe un gran número de PYMEs actualmente en México. Alrededor del 90% de las empresas mexicanas cuentan con 250 empleados o menos, lo que posiciona

[20] El informe anual completo puede encontrarse en la siguiente liga: http://www.symantec.com/es/mx/security_response/publications/threatreport.jsp
[21] Fuente: Symantec

en esta categoría. Si se considera que cada día más y más PYMEs están utilizando algún tipo de infraestructura relacionada a las Tecnologías de Información y Comunicación (TIC) se puede comprender el incremento en los ataques dirigidos a este tipo de empresas y es posible esperar un incremento en estos ataques en el corto plazo.

Debido a la condición de PYMEs, aquellas empresas que empiezan a utilizar servicios de TIC lo hacen a través de terceros, quienes les proporcionan y administran los servicios necesarios (acceso a Internet, servidores web, servidores de correo, entre otros), de tal modo que son estas empresas subcontratadas quienes ofrecen una primer línea de defensa en lo que a seguridad de información se refiere.

Sin embargo, la información requiere de varias capas de seguridad y mejora continua para que se pueda reducir al máximo posible los riesgos a los que está expuesta la información. Cuando las empresas no cuentan con controles o políticas para la seguridad de la información y sus empleados no han sido educados en materia de seguridad en Internet, las empresas se convierten en un blanco atractivo para los ciber delincuentes.

Estas características de las PYMEs muestran el porqué de un incremento en el número de ataques dirigidos y señalan la gravedad de este problema y la posibilidad de que se incremente en el corto plazo, es por esto que se consideran los siguientes ambientes controlados para ser estudiados con la metodología de investigación propuesta en este trabajo de investigación.

La aplicación de la metodología se realiza en dos casos distintos, estos casos representan los principales objetivos de los ataques dirigidos a las PYMEs, que son el robo de información y el espionaje industrial.

En el Caso A se presenta una situación donde ha ocurrido un robo de información confidencial a una PYME. Este tipo de robo puede realizarse de diferentes maneras, mencionando algunas están los robos perpetuados por un atacante que consiga penetrar en el sistema de información para robar el activo informático sin

ser detectado, o un atacante que utilice algún tipo de extorsión o engaño para conseguir el activo de información. Sin embargo, una de las amenazas más comunes es el robo o filtración de información causado por un empleado perteneciente a la empresa.

Este tipo de empleados, por lo general, no está a gusto con su trabajo, muestra apatía por las actividades que debe desarrollar y una falta de interés en general por la empresa. Lo que incrementa el peligro de esta amenaza es el conocimiento que tiene dicho empleado sobre la información que maneja la organización, conoce los procesos y procedimientos internos y toda o gran parte de la estructura empresarial, sin mencionar que además del conocimiento también posee acceso total o parcial a la información.

De tal modo que el Caso A consiste en la investigación de un robo de información que tiene como objetivo identificar a la persona responsable de dicho robo a través del análisis de un sistema detenido, es decir, sobre equipos que han sido apagados.

El Caso B presenta la investigación de un sistema perteneciente a una PYME que es víctima de espionaje industrial realizado por un competidor. Los ataques cibernéticos realizados entre empresas competidoras son bastante comunes. Las empresas buscan obtener algún tipo de ventaja en el mercado sobre sus competidores y para conseguirlo hacen uso de especialistas en seguridad de la información carentes de ética profesional, quienes llevan a cabo algún tipo de ataque para obtener información o sabotear procesos de los competidores de sus empleadores.

Los ataques relacionados con el espionaje industrial tienen como objetivo conocer los planes y proyectos de una empresa, así como el robo de propiedad intelectual.

El análisis de este Caso se realiza de manera dinámica y estática. El análisis dinámico se realiza sobre un equipo encendido y en ejecución, este tipo de análisis también es conocido como *análisis en vivo*.

4.3. Descripción del Caso A.

El Caso A presenta una red LAN que pertenece a un consultorio médico particular que ofrece diferentes servicios de salud a través de cuatro especialistas, médico general, gastroenterólogo, dermatólogo y ginecólogo. Cada especialista maneja una estación de trabajo donde guarda un registro del historial médico de cada paciente que es atendido, las estaciones de trabajo también son utilizadas para consulta de documentos especializados, uso de correo electrónico y navegación en internet.

Cada especialista cuenta con una secretaria quien lleva un control de las citas programadas, registro de los pacientes y sus historiales clínicos, así como un control de las cuentas de cada paciente. Cada secretaria utiliza su propia estación de trabajo

El consultorio cuenta con una secretaria general con su propia estación de trabajo, entre las actividades de esta persona se encuentran: manejo de la agenda de los médicos para organizar las citas con los pacientes, respaldar los expedientes de todos los pacientes, realizar un registro de la información de cada paciente. Entre las actividades extra laborales que realiza se enumera la navegación en internet y el uso de correo electrónico personal.

Esta MIPYME se encuentra en problemas ya que uno de sus clientes afirma que el consultorio ha hecho un mal uso de su información personal y amenaza con emprender acciones legales en contra del consultorio ya que ha sido víctima de un intento de extorsión a través de correo electrónico donde se utilizan los datos que proporcionó en el consultorio.

El objetivo de aplicar la metodología de investigación en este escenario es el de identificar al responsable de la fuga de información, en caso de haberla, y proporcionarle al dueño de la empresa las herramientas necesarias para tomar acciones legales si así corresponde.

4.4. Descripción del Caso B.

El caso B presenta un escenario teórico que refleja el estado de una PYME que ha sido afectada por fuga de información confidencial. La PYME en cuestión se dedica a la instalación, configuración y mantenimiento de sistemas de seguridad y vigilancia mediante circuito cerrado. La empresa ofrece sus servicios al público en general y en casos especiales a dependencias del gobierno.

Los proyectos con el gobierno involucran un proceso de licitación en el que diferentes empresas proponen el desarrollo de un proyecto en específico en donde cada una es responsable de ofrecer los productos necesarios que cumplan con los requisitos planteados en la licitación, así como su instalación y configuración. La elección de una empresa en particular, por parte de la dependencia del gobierno, se basa generalmente en la mejor propuesta en relación al costo-beneficio.

Esta PYME sospecha de una fuga de información ya que en un periodo de un mes ha perdido varias licitaciones contra una misma empresa. La primera licitación que perdieron fue pública para el desarrollo de un proyecto con una dependencia del gobierno. Sin embargo también perdieron un proyecto para particulares contra la misma empresa.

Los proyectos para particulares se realizan generalmente cuando existe un acercamiento de un cliente directamente con la empresa, la pérdida de dos clientes seguidos, quienes no tienen ninguna relación entre sí, que han contratado a la misma empresa de la competencia para desarrollar sus proyectos genera sospecha ya que ambos clientes han cancelado los avances después de recibir una propuesta de desarrollo por parte de la PYME.

Las tres propuestas para los tres proyectos que la PYME ha perdido involucran a las mismas personas en su elaboración. Estas personas son Julieta Guerrero,

dueña de la PYME, y Salvador Pedrosa, empleado de la PYME desde su creación a la fecha.

La dueña de la empresa sospecha de Salvador, quien recientemente ha mostrado inconformidad con su situación laboral. El proceso de creación de una propuesta para cualquier proyecto consiste en diseño de bocetos, cotización de precios y generación de un documento digital, es este último es en el que Salvador se involucra más ya que él es el encargado de recopilar toda la información generada para conformar el documento.

Por tal motivo, Julieta Guerrero ha solicitado los servicios de un investigador forense para examinar la estación de trabajo de Salvador en busca de evidencia de que su empleado filtra información a la competencia.

4.5. Detalles técnicos para los Casos A y B.

Las estaciones de trabajo utilizadas en los Casos A y B funcionan bajo el sistema operativo Windows en dos de sus versiones, Windows 7 Windows XP según se especifica en el desarrollo de cada Caso.

El tipo de sistema operativo usado en estos equipos es un reflejo de la situación actual de la penetración de los diferentes sistemas operativos alrededor del mundo. De acuerdo con Net Market Share[22], los sistemas operativos de la familia Windows dominan el mercado. La siguiente figura muestra la distribución de uso de los diferentes sistemas en el primer trimestre de 2014.

[22] Net Market Share es un sitio dedicado a realizar estadísticas de tecnología de Internet http://marketshare.hitslink.com/

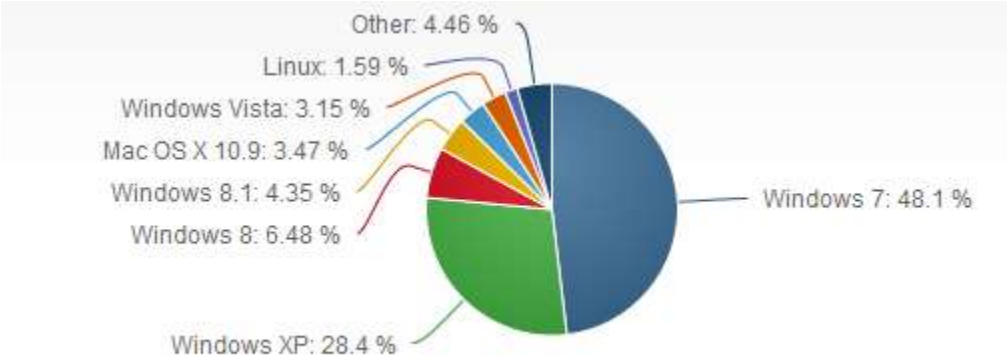


Figura 4.2 Distribución de sistemas operativos según Net Market Share[23]

En la gráfica puede observarse un claro dominio de Windows, también puede apreciarse una tendencia que muestra cómo Windows XP deja de ser sistema dominante y cede su lugar a Windows 7, tendencia que parece no se revertirá ya que Microsoft cuenta los días para dejar de brindar soporte para la plataforma XP[24].

Una fuente diferente muestra un resultado similar en la distribución de sistemas operativos, el sitio Statcounter.com[25] señala que la penetración en el mercado de Windows 7 en el periodo marzo 2013 – febrero 2014 es del 52.11%, cifra que difiere en 4.01% de Net Market Share, sin embargo la tendencia es la misma. En la figura 4.2 se muestran los valores calculados por StatCounter.

[23] Datos tomados del sitio de Net Market Share: http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpstick=0&qptimeframe=Q

[24] En el sitio oficial de soporte de Microsoft existe un contador que advierte a los usuarios de los días restantes en los que existirá soporte para Windows XP http://support.microsoft.com/kb/314865/es

[25] StatCounter es una herramienta que permite analizar el tráfico en un sitio web http://gs.statcounter.com/about

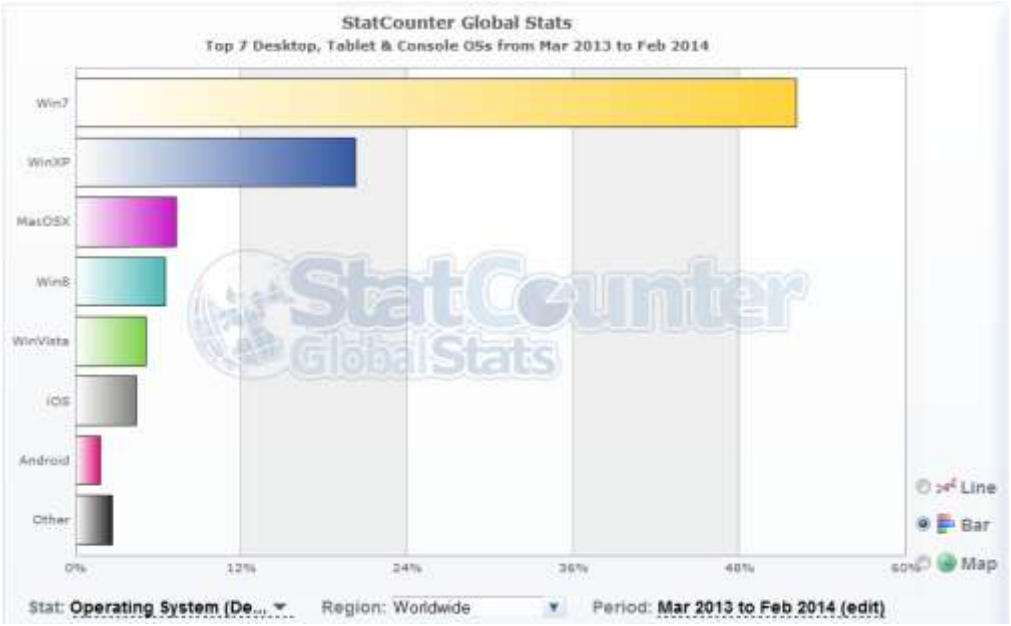


Figura 4.3 Distribución de sistemas operativos según StatCounter[26].

Ambas compañías utilizan diferentes metodologías para obtener estos resultados, cada una puede ser consultada en los sitios correspondientes[27] sin embargo la base de la recolección de los datos es el análisis de las visitas a diferentes sitios web, así como el intercambio de información entre diferentes compañías para evitar el sesgo en la información, los sistemas usados por los servidores, entre otros. Debido a la gran cantidad de dispositivos conectados a Internet, la muestra tomada por estas compañías es bastante representativa. De tal modo que la elección de las plataformas a utilizar en los ambientes controlados se apega bastante a la situación actual.

A continuación se muestra la relación del software utilizado por cada equipo utilizado en los casos A y B. (véase la tabla 4.1)

[26] Datos tomados del sitio oficial de StatCounter: http://gs.statcounter.com/#os-ww-monthly-201303-201402-bar

[27] Metodología de Net Market Share: http://marketshare.hitslink.com/faq.aspx#Methodology
Metodología de StatCounter: http://gs.statcounter.com/faq#methodology

Tabla 4.1 Relación de software instalado en las estaciones de trabajo.

Equipo 1,Caso A	Equipo 1,Caso B	Equipo 2, Caso B
Microsoft Windows Seven SP1	Microsoft Windows XP SP2 x86	Microsoft Windows XP SP2 x86
Microsoft Office 2007	Microsoft Office 2007	Microsoft Office 2007
Adobe Acrobat Reader	Adobe Acrobat Reader	Adobe Acrobat Reader
Internet Explorer	Internet Explorer	Internet Explorer
Flash Player	Mozilla Firefox	Google Chrome
-	Flash Player	Flash Player
-	WinRAR	WinRAR

La implementación de los escenarios en cada ambiente controlado se realizó a través del software de virtualización VMware, por tal motivo, los sistemas muestran procesos de este programa durante los análisis correspondientes.

En el siguiente capítulo se presenta la implementación de la metodología desarrollada para este trabajo de investigación en el Caso A.

Capítulo 5

Implementación y resultados de la metodología en el Caso A.

El capítulo 5 presenta la implementación de la metodología propuesta en este trabajo de investigación en el estudio de un caso hipotético. En este caso hipotético, denominado “Caso A”, presenta una PYME que ha sido afectada por una fuga de información confidencial, los detalles del escenario se detallan en el capítulo anterior.

La investigación en cómputo forense se centra en determinar cómo ocurrió la fuga de información y tratar de identificar un responsable.

Las actividades realizadas cubren todas las etapas presentadas en la metodología, desde la etapa de preparación, donde se definen los lineamientos para la creación de una estación de investigación, hasta la etapa de presentación, en la cual se ofrecen los resultados de la investigación de manera estructurada.

En las etapas de identificación, preservación y análisis se documenta cada actividad realizada según lo propuesto en la metodología, generando formatos y otros documentos que son incluidos en los anexos correspondientes.

A continuación, la aplicación de la metodología para la investigación de delitos informáticos en el *Caso A*.

5.1. Etapa de preparación.

De acuerdo con la metodología establecida en este trabajo de investigación, el primer paso a desarrollar es el proceso de preparación, el cual consiste en dos fases:

1. Preparación de una estación de trabajo a utilizarse en la investigación.

La estación de trabajo debe tener las herramientas de software necesarias para realizar labores de cómputo forense, así como el hardware necesario para respaldar y soportar las diferentes aplicaciones. Para esta investigación se utiliza un equipo con el sistema operativo Microsoft Windows 7 SP1 de 64 bits. Entre las

aplicaciones instaladas[28] se encuentra FTK Imager, los datos de la aplicación se documentan en el formato PREIN-APP-01 (véase la tabla 5.1):

Tabla 5.1 Datos sobre la aplicación FTK Imager.

Formato: PREIN-APP-01	
Nombre de la aplicación	FTK Imager
Desarrollador	AccessData
Versión	3.1.3.
Hash MD5 del instalador	27868c05d6c0543fff9fe3f5b80d0e2e
Hash MD5 del ejecutable	f6d2c8f47461e589410a17c097c29385
Fuente de descarga	http://www.accessdata.com/support/product-downloads
Fecha de instalación	15/01/2013

2. Esterilización de dispositivos de almacenamiento.

Para alojar las imágenes forenses, hallazgos relevantes para la investigación y otros archivos, respaldos, entre otros, se preparan dispositivos de almacenamiento, esterilizándolos con la intención de eliminar cualquier dato que estuviera alojado en él. La documentación de este proceso se muestra en el formato PREIN-EDA-01 (véase la tabla 5.2):

[28] Al ser una muestra del uso de la metodología, no se listan las características de todas las aplicaciones instaladas por cuestiones de practicidad. Se recomienda ampliamente que en una situación real se documente todas las aplicaciones usadas.

Tabla 5.2 Información sobre la esterilización del dispositivo.

Formato: PREIN-EDA-01	
Información del dispositivo	
Marca/modelo	Adata/HD710
Número de serie	ADATA-4891943898
Capacidad	1.0 TB
Descripción	Disco duro externo con interfaz USB 3.0
Información sobre la esterilización	
Aplicación utilizada	Clean Disk Security
MD5 de la aplicación	54868c05d6c0543aaf9fe3f5c00d0e1b
Algoritmo utilizado	NIS
Número de pasadas	7
Fecha y hora de la esterilización	06/05/2013
Responsable de la esterilización	Demian García
Firma del responsable	

5.2. Etapa de identificación.

Una vez terminado el proceso de preparación, el primer paso a seguir es conseguir la autorización correspondiente para iniciar la investigación. A continuación se presenta la carta de autorización:

Carta de Autorización de Inicio de la Investigación
Fecha: 7 de mayo de 2013 Por medio de la presente se concede autorización expresa por parte del representante de la empresa **Consultorio Médico AC**, **Dr. Carlos Fernández**, al equipo de investigación liderado por, **Demian García**, para iniciar a la investigación en cómputo forense con identificador: **Caso A-201305-CMAC**. La investigación contempla la revisión de la estación de trabajo **HP/Desktop2510** con número de serie: **HP-p314248.** Con disco duro marca: **Western Digital** modelo: **WD2012** con capacidad de: **80GB** y número de serie: **152D20337A0C.** Así mismo, el representante de la empresa se compromete a apoyar y proveer todas las facilidades necesarias al equipo de investigación para que éste pueda llevar cabo la tarea sin complicaciones. _____ _____ Firma del representante de la empresa Firma del líder de la investigación.

Una vez que la misiva ha sido firmada por las partes correspondientes, se hace entrega de la carta de confidencialidad:

Carta de Confidencialidad.

Fecha: 7 de mayo de 2013

Por medio de la presente, el equipo de investigación liderado por **Demian García** se compromete a respetar la privacidad de la información, relacionada con la empresa **Consultorio Médico AC**, al considerarla como estrictamente confidencial y de uso exclusivo a los procesos relacionados con la investigación en cómputo forense **Caso A-201305-CMAC** , por lo cual, el equipo de investigación integrado por **Demian García** se abstendrá a divulgarla, publicarla, distribuirla a terceros, utilizarla en provecho propio, y de conservar copias, respaldos totales o parciales, ya sean electrónicos o físicos, sin la autorización del representante de la empresa.

_____	_____
Nombre y firma del líder de la investigación	Nombre y firma del representante de la empresa

Cuando las cartas han sido firmadas se recopila la información del personal que conforma al equipo de investigación, esta información se recopila en el formato IDE-IEF-01 (véase la Tabla 5.3)

Tabla 5.3 Información de los integrantes del equipo asignado a la investigación.

Formato: IDE-IEF-01	
Identificador del investigador	IEF-DRGV-19981101
Nombre	Demian García
Rol en la investigación	Líder de la investigación

Firma	
Identificación con fotografía	

El siguiente paso es recopilar información relacionada a la empresa, al incidente de seguridad, la atención del incidente y otros puntos interés. Toda la información recopilada es almacenada en diferentes formatos, lo que facilita futuras consultas. El formato IDE-INV-Caso A-201305-CMAC recopila información general sobre la investigación (véase la Tabla 5.4).

Tabla 5.4 Información general acerca de la investigación.

Formato: IDE-INV-Caso A-201305-CMAC	
Identificador de la investigación	Caso A-201305-CMAC
Tipo de incidente	Fuga de información confidencial. Se pretende determinar al responsable.
Activo afectado	Información personal y financiera de pacientes del Consultorio Médico (nombres, direcciones, datos de contacto, números de cuenta, entre otros).
Fecha de inicio	7 de mayo de 2013
Investigador asignado	Demian García
Datos generales de la empresa afectada	
Nombre	Consultorio Médico AC
Giro	Consultorio Médico
Dirección	Calle 4 Col. Del Valle, Delegación Miguel Hidalgo, Distrito Federal, México.
Director General	Dr. Carlos Fernández
Contacto	cfernarndez@gmail.com tel 55-213-445 cel 044-55-432-445-10

El día 7 de mayo de 2013 el Dr. Carlos Fernández ha solicitado una investigación basada en cómputo forense para determinar al responsable de la fuga de información confidencial relacionada a los pacientes del Consultorio Médico AC.

La solicitud de esta investigación es generada por la amenaza de una posible demanda por parte de un paciente quien asegura que un tercero ha hecho mal uso de la información personal y financiera que otorgó al Consultorio Médico AC.

Los datos personales que el paciente menciona que han sido mal utilizados son: nombre, teléfono y dirección. El paciente menciona que ha recibido llamadas telefónicas que le ofrecen tratamientos para la enfermedad que padece. El argumento que soporta la acusación contra el Consultorio Médico AC (CMAC) es que nadie más conoce de su padecimiento.

Siendo esta la única información disponible al inicio de la investigación es necesario recopilar más datos entrevistando al personal que está involucrado con el incidente de forma directa o indirecta. Antes de iniciar la entrevista se documenta la información del personal[29] como se muestra en la Tabla 5.5.

Tabla 5.5 Información de los empleados de la empresa afectada.

Formato: IDE-ISE-01	
Empleado 1	
Nombre	Erika Lucio
Puesto	Secretaria del CMAC
Descripción de actividades	Manejo de las cuentas del consultorio, orientación a pacientes, captura de datos a nuevos pacientes, manejo de los pagos de todos los pacientes, acceso a internet y correo electrónico.
Firma	
Identificación con fotografía	
Empleado 2	
Nombre	Dr. Carlos Fernández

[29] Muestra de la información documentada, en un caso real se debe recopilar la información de todo el personal.

Puesto	Médico general
Descripción de actividades	Atención a pacientes, manejo de historiales clínicos, consulta de documentos especializados, uso de Internet y correo electrónico.
Firma	
Identificación con fotografía	
Todas personas mencionadas en este documento al momento de firmarlo aceptan que la información aquí recabada es verídica.	

Las preguntas incluidas en la entrevista son:

a) ¿Qué **activo informático** se vio afectado en el incidente de seguridad?

b) ¿Dónde se encuentra alojado dicho activo (ubicación física del dispositivo)?

c) ¿Quién es el responsable del equipo en el que el activo se encuentra alojado?

d) ¿Quién tiene acceso a tal equipo?

e) ¿El equipo se encuentra conectado a una red?, de ser así ¿Cuál es la información relacionada con la red?

El resultado de la entrevista se documenta en los formatos IDE-AIT-01 (véase la Tabla 5.6), IDE-HW-01 (véase la Tabla 5.7),y IDE-RED-01 (véase la Tabla 5.8).

Tabla 5.6 Información relacionada al activo de información afectado.

Formato: IDE-AIT-01	
Identificador del activo	AIT-001
Tipo de activo	Archivo de texto que contiene registro de información personal de pacientes.
Extensión	Posiblemente .xls o .xlsx
Software asociado	Microsoft Excel
Descripción	Lista con datos personales de los pacientes. Contiene nombres, teléfonos, direcciones, género, fecha de ingreso al consultorio, especialidad,

	número de cuenta, número de expediente, número de paciente.
Usuarios con acceso al archivo	Erika Lucio
Equipo en el que está ubicado	PC-009
Responsable del activo	Erika Lucio.

Tabla 5.7 Información sobre el equipo que almacena el activo afectado.

Formato: IDE-HW-01	
Tipo de dispositivo	Estación de Trabajo (PC)
Identificador del dispositivo	PC-009
Marca/Modelo	HP/Desktop2510
Número de serie	HP-p314248
Características Generales	Gabinete color negro.
Disco Duro asociado al equipo(1)	
Identificador del disco duro	PC-009-DD01
Marca	Western Digital
Modelo	WD2012
Número de serie	152D20337A0C
Capacidad de almacenamiento	80GB
Tipo de Interfaz	IDE
Ubicación del equipo	
Área a la que pertenece	Administración general del consultorio
Empresa/Organización	Consultorio Médico AC
Dirección	Calle 4 Col. Del Valle, Delegación Miguel Hidalgo, Distrito Federal, México.
Información adicional	Equipo ubicado en la recepción del consultorio.
Responsable del equipo	
Nombre del responsable	
Nombre de usuario	Erika Lúcio
Puesto	Secretaria del consultorio
Correo electrónico	elucio@outlook.com, consul-med-ac@outlook.com
Teléfono	55-213-445
Descripción de actividades	Manejo de las cuentas del consultorio, orientación a pacientes, captura de datos a nuevos pacientes, manejo de los pagos de todos los pacientes, acceso a internet y correo electrónico.
Conectividad	
Red a la que se conecta el equipo	Red Consultorio

Tipo de conexión	Ethernet
Software	
Sistema operativo	Microsoft Windows Seven SP1

Tabla 5.8 Información sobre la red a la que está conectado el equipo.

Formato: IDE-RED-01	
Tipo de red	LAN
Tipo de conexión	Ethernet
Topología de red	Estrella
Número de equipos conectados	9
ISP	Uninet
Administrador de la red	
Nombre	---
Correo	---
Tel	---
Comentario	No hay personal asignado a la administración de la red.

El resultado del proceso de entrevista señala que el activo afectado es una lista con los datos de cada paciente, estos datos son: nombre, fecha de nacimiento, domicilio, teléfono, correo electrónico, número de cuenta, sexo, clave del historial, fecha de ingreso, y especialidad. Este archivo es manejado únicamente por la Secretaria del CMAC Erika Lucio. Ningún otro empleado maneja este tipo de información.

Con la información recabada hasta el momento, es posible plantear una primera hipótesis: es posible que la fuga de información se haya dado a través de correo electrónico si se considera que solo existe un usuario que genera y tiene acceso a la información confidencial en cuestión, y que ese empleado cuenta con acceso a Internet y hace uso del servicio de correo electrónico.

5.3. Etapa de preservación.

Para probar la hipótesis es necesario analizar el sistema en busca de evidencia que demuestre que la fuga de información se presentó bajo las condiciones planteadas. Sin embargo, antes de iniciar el análisis la metodología marca el inicio del proceso de cadena de custodia. La información general de este proceso se documenta en el formato PRE-CC-01 (véase la Tabla 5.9).

Tabla 5.9 Información general sobre la cadena de custodia.

Formato: PRE-CC-01	
Identificador de la cadena de custodia	PRE-CC-01
Identificador de la investigación	Caso A-201305-CMAC
Identificador del custodio asignado	ICF-DGV-201305
Descripción de los dispositivos	Disco duro de 80 GB que contiene sistema operativo y datos del usuario Erika Lucio.
Datos del dispositivo	
Identificador del dispositivo	PC-09-DD01
Bitácora asociada	LOG-CC-01
Fecha y hora de inserción a la cadena	07/05/2013 16:00hrs

Para cada dispositivo custodiado se debe documentar todos y cada uno de los accesos al mismo, para ello se utiliza una bitácora como se muestra en la Tabla 5.10:

Tabla 5.10 Bitácora de acceso al dispositivo PC-09-DD01.

Bitácora : *LOG-CC-01* correspondiente al dispositivo: *PC-09-Dd01* perteneciente a la Cadena de custodia: *PRE-CC-01* de la Investigación: *Caso A-201305-CMAC*							
Nombre y procedencia del solicitante	Motivo	Traslado	Fecha y hora de inicio	Fecha y hora de término	Firma	Autorizado por	Firma
Demian García, Líder de la	Obtención de imagen forense	Sin traslado	07/05/2013 17:00 hrs	07/05/2013 18:35hrs		Demian García, Custodio	

investigación						de la Cadena	
Demian García, Líder de la investigación	Obtención de una segunda imagen forense	Sin traslado	07/05/2013 19:00hrs	07/05/2013 20:55hrs		Demian García, Custodio de la Cadena	

Para realizar la imagen forense se utilizó la herramienta FTK Imager 3.1.20 la figura 5.1 se muestra la interfaz principal de la herramienta.

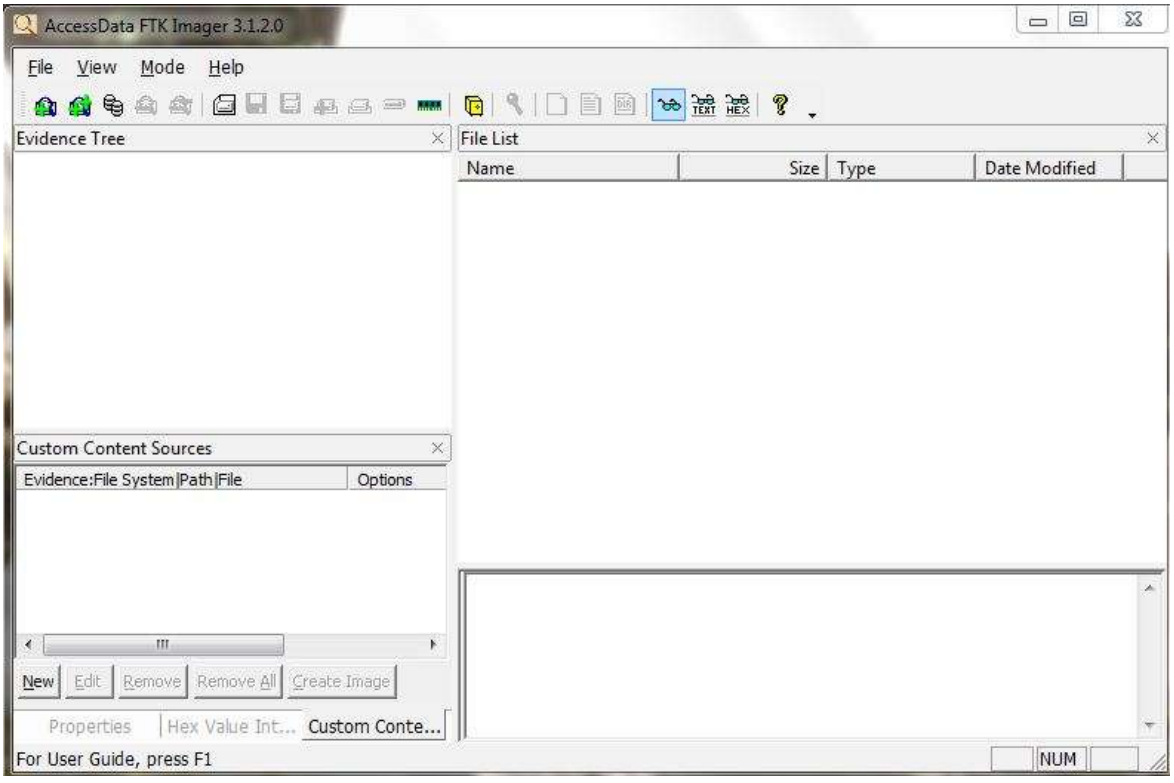


Figura 5.1 Interfaz principal de FTK Imager.

Para crear la imagen es necesario indicar la fuente que ha de ser copiada, en el menú "*file*" se selecciona la opción "*Create Disk Image*…" y se selecciona el tipo de dispositivo fuente a copiar. En este caso es de tipo "*Physical Drive*" y está conectado a través del puerto USB. La figura 5.2 muestra las ventanas correspondientes para los procedimientos antes mencionados.

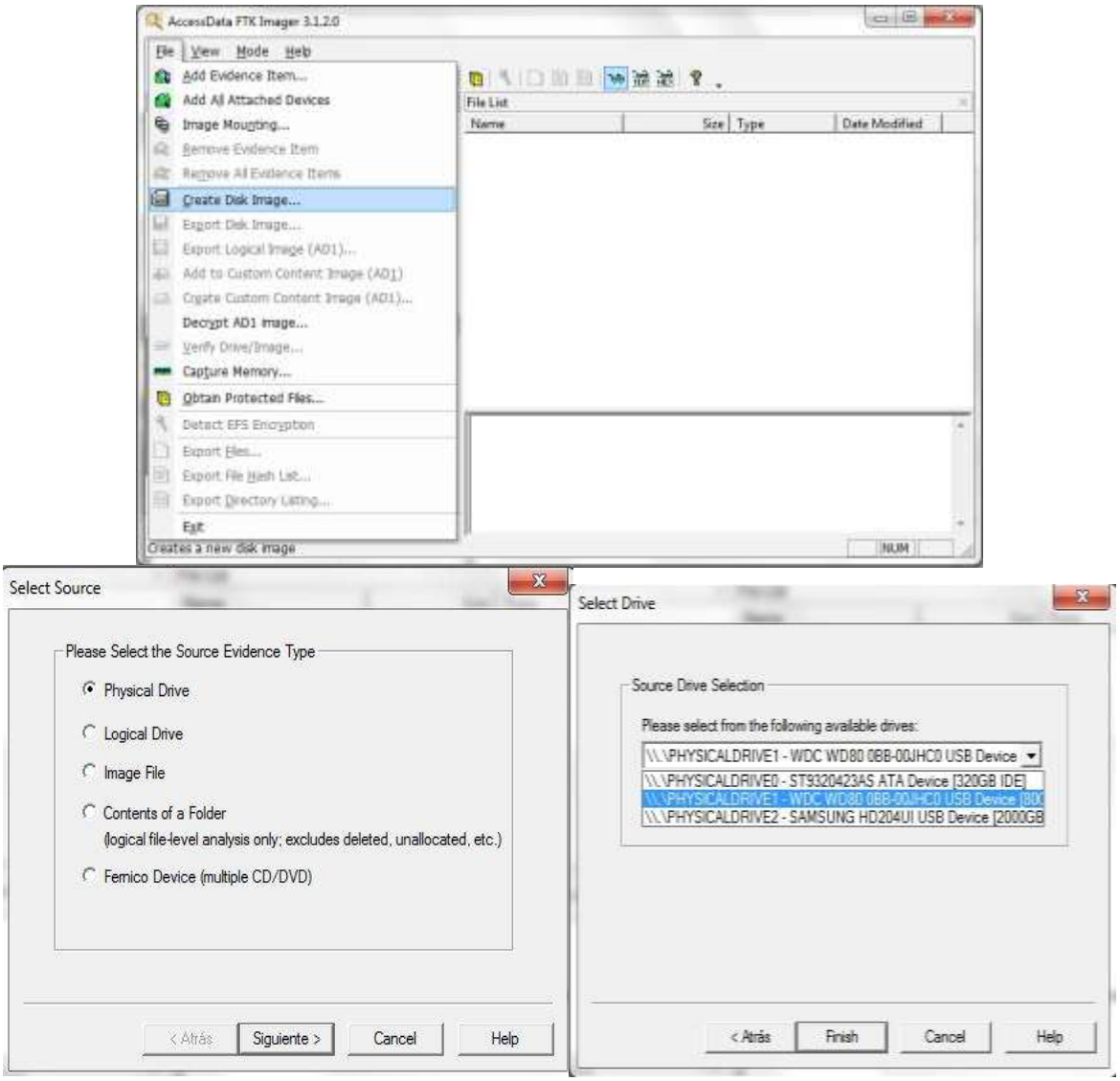


Figura 5.2 Selección de tipo de dispositivo origen.

Una vez que se selecciona el dispositivo orignal se debe elegir el tipo de archivo para la imagen forense, en este caso se eligió la extención ".E01".

La hermienta FTK permite fragmentar la imagen forense en diferentes archivos de un tamaño establecido por el usuario, en este caso no se utilizó la fragmentación y se generó un sólo archivo. La figura 5.3 muestra la venta con las opciones para guardar la imagen forense.

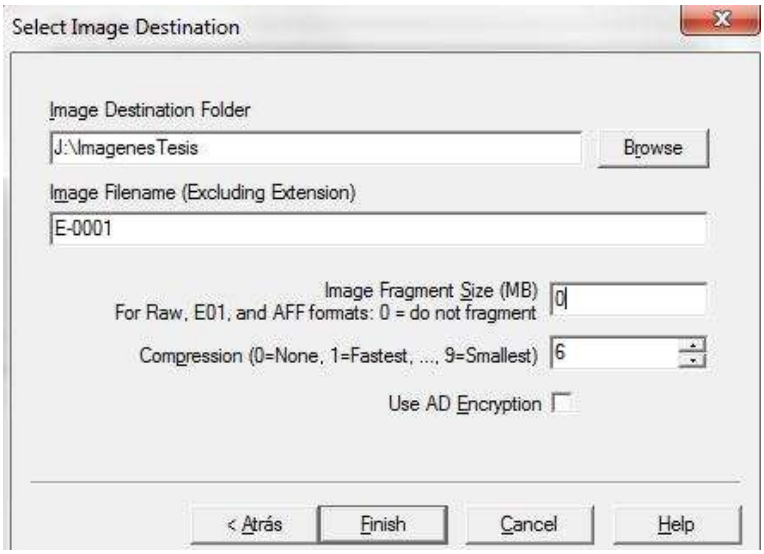


Figura 5.3 Selección del destino de la imagen y tamaño de los fragmentos.

Una vez que el proceso de copiado haya terminado, la herramienta genera un archivo con el resumen de la operación realizada. Toda la información relacionada con este proceso debe ser asentada en el formato correspondiente (véase la Tabla 5.11) para contar con un respaldo por escrito de las acciones realizadas.

Tabla 5.11 Resumen proceso de generación de imagen forense.

Formato: PRE-GIF-01	
Identificadores	
Identificador de la imagen forense	IMGF-PC-009-DD01
Identificador del dispositivo origen	PC-009-DD001
Identificador de la cadena de custodia a la que pertenece el dispositivo	CC-001
Identificador del dispositivo donde se aloja la imagen	ED-001
Información de la generación de la imagen	
Herramienta usada	FTK Imager
MD5 de la herramienta	f6d2c8f47461e589410a17c097c29385
MD5 de la imagen generada	ef6a7ab2afb99dfdb3218f9d35998130

Formato de la imagen	.E01
Tamaño de la imagen	81GB
Responsable de la generación del a imagen	Demian García
Firma del responsable	
Hora y fecha de la generación	07 mayo 2013, 17:00hrs
Identificado de la bitácora de hashes	HASH-PC-009-DD001

5.4. Etapa de análisis.

Una vez que se ha generado la imagen forense es posible analizarla con la herramienta FTK Imager, entre las ventajas que presenta esta herramienta es que no modifica la evidencia y ofrece una forma cómoda de visualizar la información contenida en la imagen forense.

Para visualizar el contenido de la imagen es necesario utilizar la opción “añadir evidencia” y seleccionar la opción “archivo de imagen” como se muestra en la figura 5.4.

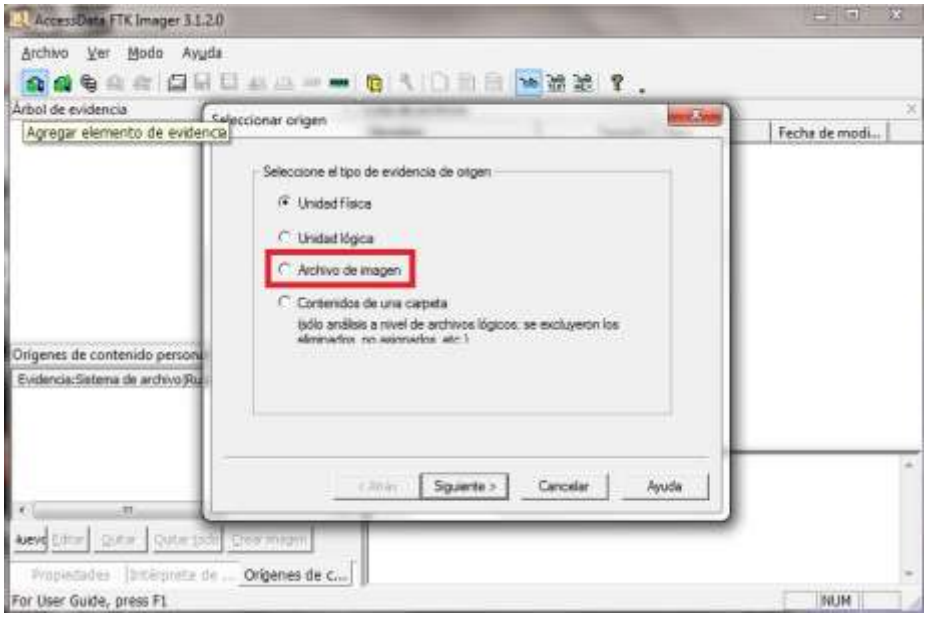


Figura 5.4 Evidencia, archivo tipo imagen.

Cuando la imagen forense es montada correctamente en la herramienta, la ventana principal muestra las particiones existentes en la evidencia y el espacio no particionado en el lado izquierdo, mostrando la información como un **árbol de directorios**. La figura 5.5 muestra la vista de la evidencia montada en la herramienta.

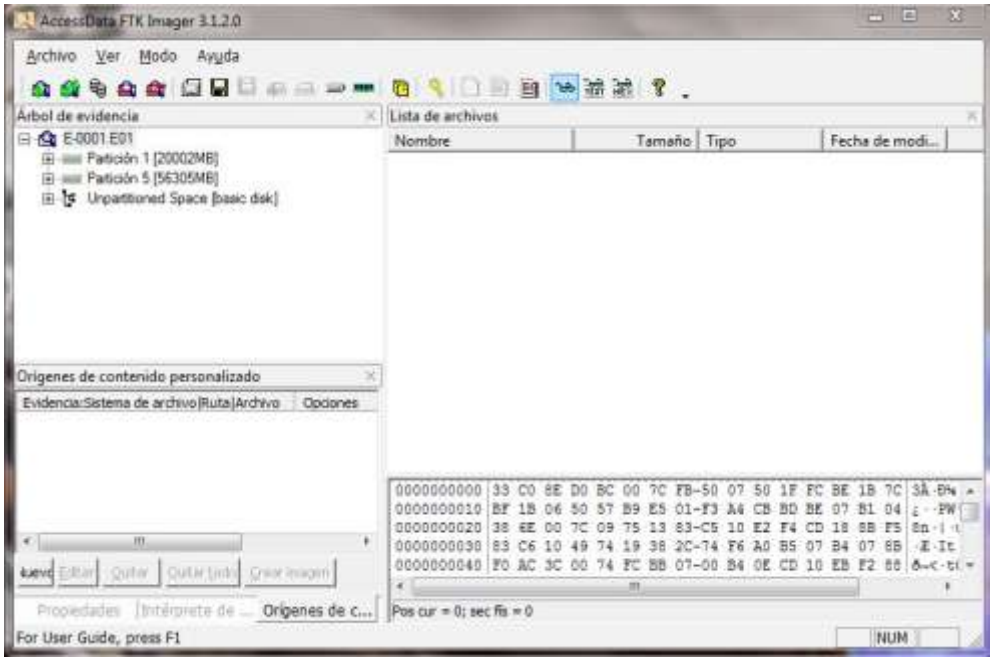


Figura 5.5 Evidencia correctamente montada.

Al montar correctamente la imagen forense es posible iniciar el análisis en busca de evidencia que apoye la hipótesis que plantea que la fuga de información se perpetró mediante el uso del correo electrónico.

Para comprobar esta teoría es necesario ubicar los archivos de correo electrónico en la imagen forense. De manera predeterminada los archivos de correo del sistema Microsoft Outlook, el cual es usado por la empleada en cuestión, se encuentran en el directorio C:*Documents and Settings**Consultorio**Configuración local**Datos de programa**Microsoft**Outlook*\ y utilizan la extensión ".pst". En la figura 5.6 se muestra el árbol de directorios del lado izquierdo desplegando la ruta antes mencionada, mientras que en el panel derecho se muestra el contenido del directorio, así como información adicional.

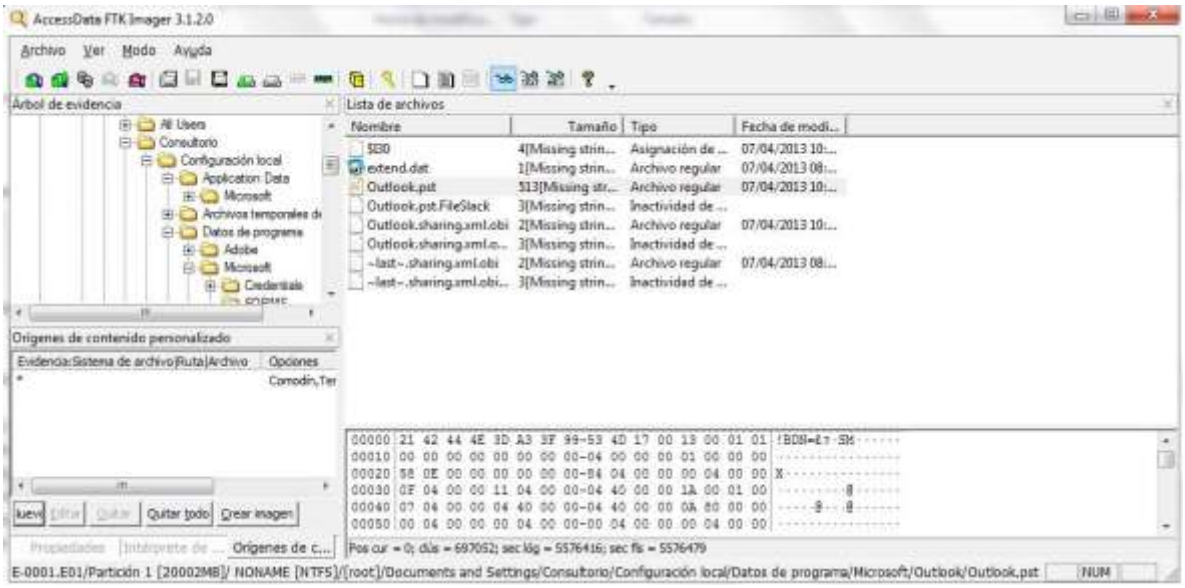


Figura 5.6 Contenido del directorio de Microsoft Outlook.

Una vez que se ha identificado el archivo “Outlook.pst” es necesario recuperarlo para revisar su contenido. La herramienta FTK Imager permite exportar el archivo para manipularlo fuera de la imagen forense. La figura 5.7 muestra este procedimiento.

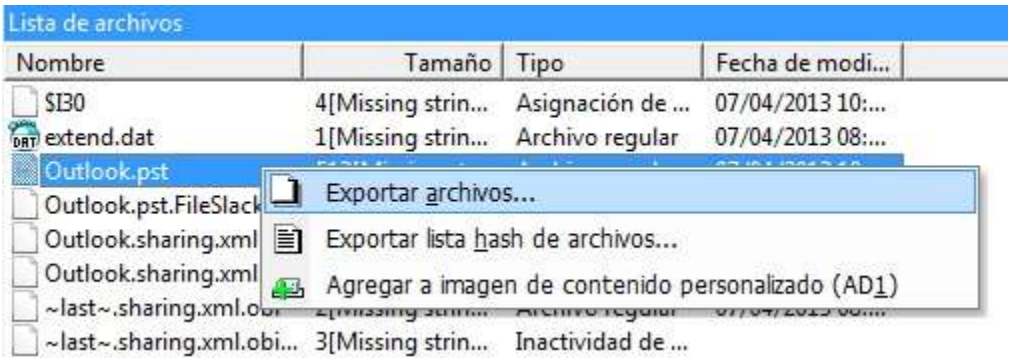


Figura 5.7 Exportación del archivo Outlook.pst.

Exportar el archivo permite analizarlo sin alterar la evidencia obtenida hasta ahora, la imagen forense, pero es necesario comprobar que se trata del mismo archivo, el exportado y el contenido en la imagen forense. Para ello se realiza una comprobacion del hash MD5.

La herramienta FTK Imager proporciona un valor de hash MD5 para el archivo en cuestión:

Archivo: E-0001.E01\Partición 1 [20002MB]\ NONAME [NTFS]\[root]\Documents and Settings\Consultorio\Configuración local\Datos de programa\Microsoft\Outlook\Outlook.pst
Hash MD5: 220127f1f1b2bc8e268966a5fa152379

Al realizar el cálculo del hash con otra herramienta se obtiene lo siguiente:

Figura 5.8 Hash MD5 del archivo Outlook.pst.

Como puede observarse, ambos valores MD5 son iguales, lo que significa que el archivo no sufrió ninguna modificación al ser exportado de la imagen forense, por lo que es posible revisar su contenido con la seguridad de que la información encontrada en él es válida. El siguiente paso es documentar el hallazgo basándose en el formato ANA-HED-01 (véase la Tabla 5.12).

Tabla 5.12Información sobre el hallazgo “Outlook.pst”.

Formato ANA-HED-01	
Identificador de la imagen forense	IMGF-PC-009-DD01
Identificador del hallazgo	HED-01-PC-009-DD01
Nombre del hallazgo (archivo)	Outlook.pst
Ubicación del hallazgo (archivo)	C:\Documents and Settings\Consultorio\Configuración local\Datos de programa\Microsoft\Outlook\
Hash MD5 del hallazgo	220127f1f1b2bc8e268966a5fa152379
Descripción	Archivo que contiene el correo electrónico

	configurado para la cuenta de usuario "Consultorio" utilizada por la secretaria
Identificador del dispositivo de almacenamiento usado para copiar el hallazgo	ED-001

Para analizar el contenido del archivo "Outlook.pst" se requiere del uso de alguna aplicación ya que es un formato de archivo propietario. Es posible utilizar la aplicación Microsoft Outlook, sin embargo se requiere de un ambiente controlado del cual pueda garantizarse que no altera la evidencia al agregarla al sistema.

Para evitar complicaciones innecesarias se utiliza la aplicación PSTViewer Pro 4 para visualizar el archivo. La figura 5.9 muestra la interfaz de la aplicación con el archivo "Outlook.pst" cargado para su visualización.

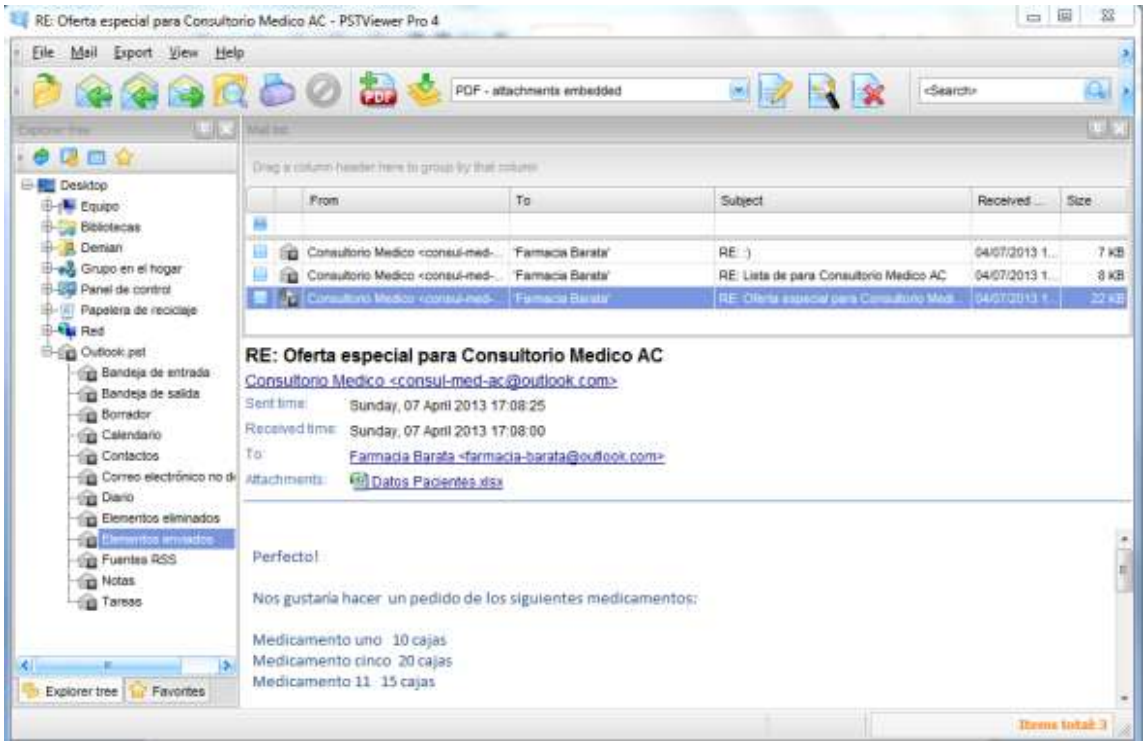
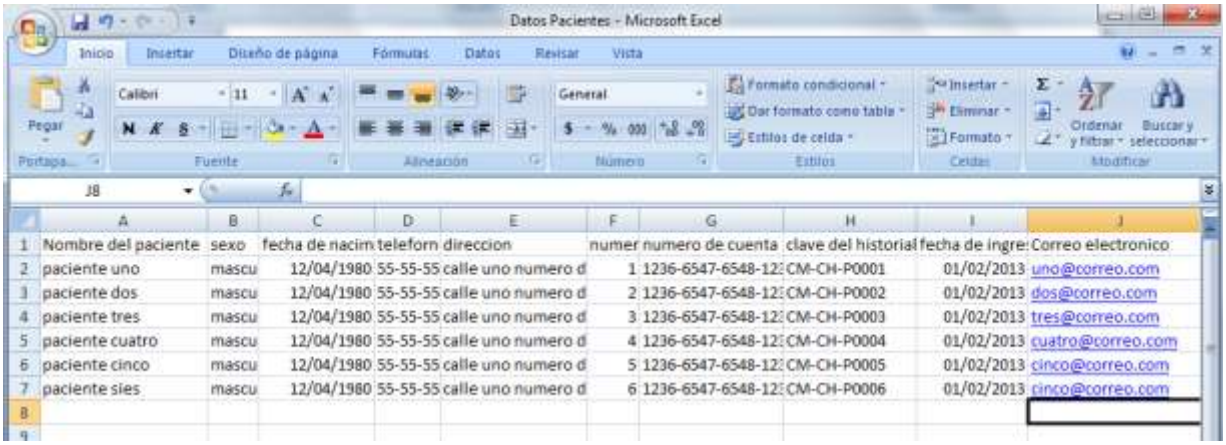


Figura 5.9 Interfaz de PSTViwer Pro 4.

En el archivo de correo puede apreciarse una conversación con la cuenta de correo farmacia-barata@outlook.com en la que se ofrece un descuento en medicamentos a cambio de datos de los pacientes del consultorio.

En el archivo se encuentra un correo enviado el 7 de abril de 2013 con un archivo adjunto llamado “Datos Pacientes.xlsx”. Al recuperar el archivo y abrirlo se puede apreciar la información confidencial de los pacientes. La figura 5.10 muestra el contenido del archivo.



	A	B	C	D	E	F	G	H	I	J
1	Nombre del paciente	sexo	fecha de nacim	teleform	direccion	numer	numero de cuenta	clave del historial	fecha de ingre	Correo electronico
2	paciente uno	mascu	12/04/1980	55-55-55	calle uno numero d	1	1236-6547-6548-12	CM-CH-P0001	01/02/2013	uno@correo.com
3	paciente dos	mascu	12/04/1980	55-55-55	calle uno numero d	2	1236-6547-6548-12	CM-CH-P0002	01/02/2013	dos@correo.com
4	paciente tres	mascu	12/04/1980	55-55-55	calle uno numero d	3	1236-6547-6548-12	CM-CH-P0003	01/02/2013	tres@correo.com
5	paciente cuatro	mascu	12/04/1980	55-55-55	calle uno numero d	4	1236-6547-6548-12	CM-CH-P0004	01/02/2013	cuatro@correo.com
6	paciente cinco	mascu	12/04/1980	55-55-55	calle uno numero d	5	1236-6547-6548-12	CM-CH-P0005	01/02/2013	cinco@correo.com
7	paciente sies	mascu	12/04/1980	55-55-55	calle uno numero d	6	1236-6547-6548-12	CM-CH-P0006	01/02/2013	cinco@correo.com
8										
9										

Figura 5.10 Contenido del archivo “Datos Pacientes.xlsx”.

El hallazgo del archivo es documentado en el formato ANA-HED-02 (véase la Tabla 5.13).

Tabla 5.13 Información sobre el hallazgo “Datos Pacientes.xlsx”.

Formato: ANA-HED-02	
Identificador de la imagen forense	IMGF-PC-009-DD01
Identificador del hallazgo	HED-01-PC-009-DD02
Nombre del hallazgo (archivo)	Datos Pacientes.xlsx
Ubicación del hallazgo (archivo)	C:\Documents and Settings\Consultorio\Configuración local\Datos de programa\Microsoft\Outlook\
Hash MD5 del hallazgo	220127f1f1b2bc8e268966a5fa152379
Descripción	Archivo de texto que contiene información

	confidencial enviado a una cuenta de correo ajena al Consultorio Médico AC.
Identificador del dispositivo de almacenamiento usado para copiar el hallazgo	ED-001

De esta forma se determina que el día 7 de abril de 2013 la cuenta de correo consul-med-ac@outlook.com envió el archivo "Datos Pacientes.xlsx" el cual contiene información confidencial de los pacientes a la cuenta farmacia-barata@outlook.com, cuenta externa al consultorio a cambio de descuentos en medicinas.

De acuerdo al formato IDE-HW-01, referente a los datos de la estación de trabajo con identificador *PC-09* que utiliza el disco duro con identificador *PC-09-DD01*, el cual contiene el hallazgo analizado, la persona con acceso a la cuenta consul-med-ac@outlook.com es Erika Lucio, secretaria del consultorio.

5.5. Etapa de presentación.

Esta etapa resume todo el proceso de investigación resaltando los puntos más sobresalientes y expone los resultados de las actividades realizadas para corroborar la hipótesis planteada.

La presentación de resultados incluye:

- Antecedentes
- Informe ejecutivo
- Actividades realizadas
    - Generación de imagen forense
    - Ubicación de registros de correo
    - Extracción de los registros de correo

    - Análisis de los registros de correo
- Recomendaciones
- Conclusiones

5.5.1. Antecedentes.

El día 7 de mayo de 2013 se reportó una fuga de información confidencial, entre los datos afectados se encuentran registros de la información personal y financiera de los pacientes del Consultorio Médico AC. La fuga de información fue reportada por el Dr. Carlos Fernández quien solicitó una investigación en cómputo forense para determinar al responsable de la filtración de los datos.

5.5.2. Informe ejecutivo.

Los datos personales y financieros de los clientes del Consultorio Médico AC fueron enviados por correo electrónico desde la cuenta "consul-med-ac@outlook.com". De acuerdo a la información proporcionada por los empleados del consultorio, el responsable de esa cuenta de correo es la secretaria Erika Lucio.

Los datos de los clientes fueron enviados en un archivo de Excel, DatosPacientes.xlsx, a la cuenta de correo "farmacia-barata@outlook.com" el día 7 de abril de 2013 a las 17:08.

5.5.3. Actividades realizadas.

La investigación fue realizada por Demian García, y toda la documentación correspondiente se encuentra en el expediente Caso A-201305-CMAC. Durante la investigación se realizaron las siguientes actividades:

- Generación de una imagen forense del sistema afectado.
- Ubicación de los registros del correo electrónico.

- Extracción del archivo de registros del correo electrónico.
- Análisis de los registros del correo electrónico.

5.5.3.1 Generación de imagen forense.

La investigación se centró en el análisis del contenido del disco duro de la estación de trabajo utilizada por la secretaria Erika Lucio. El equipo fue registrado en el formato IDEN1A-HW-001-Caso A-201305-CMAC y se le asignó el identificador PC-009, al disco duro utilizado en el equipo se le asignó el identificador PC-009-DD01.

El disco duro contiene archivos del sistema operativo y archivos del usuario, para la generación de la imagen forense se utilizó la herramienta FTK Imager, la información de este proceso se encuentra documentada en el formato PRE-GIF-01 (véase la tabla 5.14)

Tabla 5.14 Información sobre la generación de la imagen forense.

Formato: PRE-GIF-01	
Identificadores	
Identificador de la imagen forense	IMGF-PC-09-DD01
Identificador del dispositivo origen	PC-09-DD001
Identificador de la cadena de custodia a la que pertenece el dispositivo	LOG-CC-01
Información de la generación de la imagen	
Herramienta usada	FTK Imager
MD5 de la herramienta	f6d2c8f47461e589410a17c097c29385
Identificador del dispositivo donde se aloja la imagen	ED-001
MD5 de la imagen generada	ef6a7ab2afb99dfdb3218f9d35998130
Formato de la imagen	.E01
Tamaño de la imagen	81GB
Responsable de la generación del a	Demian García

imagen	
Firma del responsable	
Hora y fecha de la generación	07 mayo 2013, 17:00hrs
Identificado de la bitácora de hashes	HASH-PC-009-DD001

La imagen forense resultante fue almacenada en el dispositivo esterilizado con identificador ED-001, el formato PRE-GIF-01 contiene toda información relacionada a la generación de dicha imagen. Es importante mencionar que el acceso al dispositivo fuente y a la imagen forense fue estrictamente controlado y documentado en cada momento de la investigación. La documentación puede encontrarse en el formato PRE-DCC-01 y en la bitácora de acceso PRE-BAD-01.

5.5.3.2. Ubicación de registros de correo electrónico.

Durante la investigación se utilizó únicamente la imagen forense, en la cual se ubicó el archivo "C:*Documents and Settings**Consultorio**Configuración local**Datos de programa**Microsoft**Outlook**Outlook.pst"* el cual contiene información relacionada a la cuenta de correo "consul-med-ac@outlook.com", entre la información que contiene se encuentran los correos envidos y recibidos, agenda de contactos, entre otros. La imagen 2.2.1 muestra el contenido del directorio "C:*Documents and Settings**Consultorio**Configuración local**Datos de programa**Microsoft**Outlook**"* el cual incluye al archivo "Outlook.pst" (véase la figura 5.11).

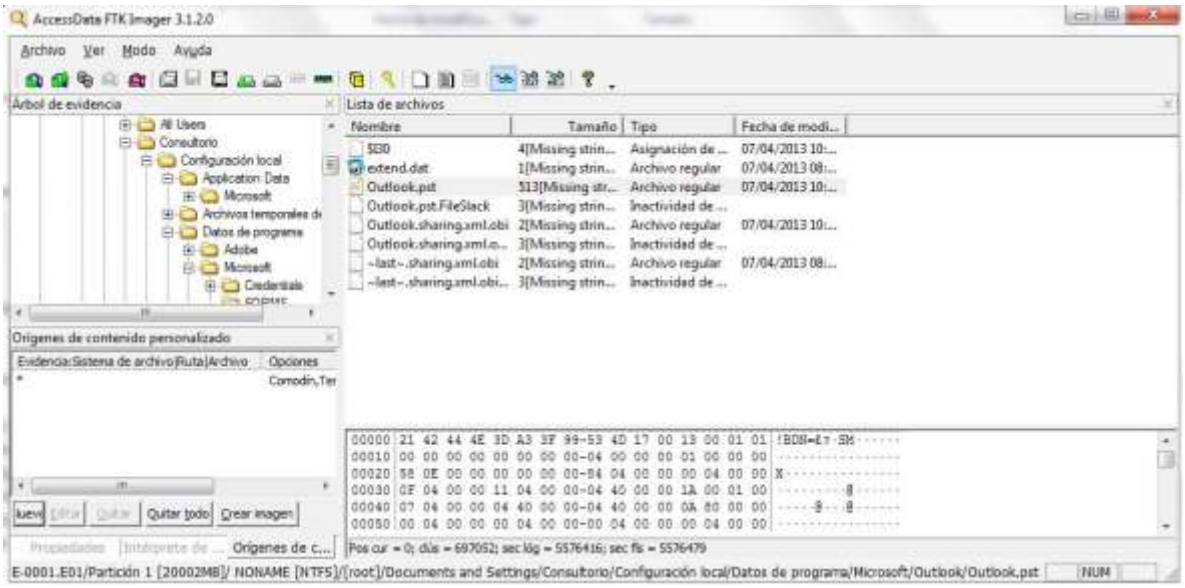


Figura 5.11 Registros de correo electrónico en la imagen forense.

5.5.3.3. Extracción de los registros de correo.

A través de la herramienta FTK Imager se extrajo el archivo “Outlook.pst” de la imagen forense para su análisis en un ambiente controlado. La figura 5.12 muestra la extracción del archivo a través de la herramienta FTK Imager.

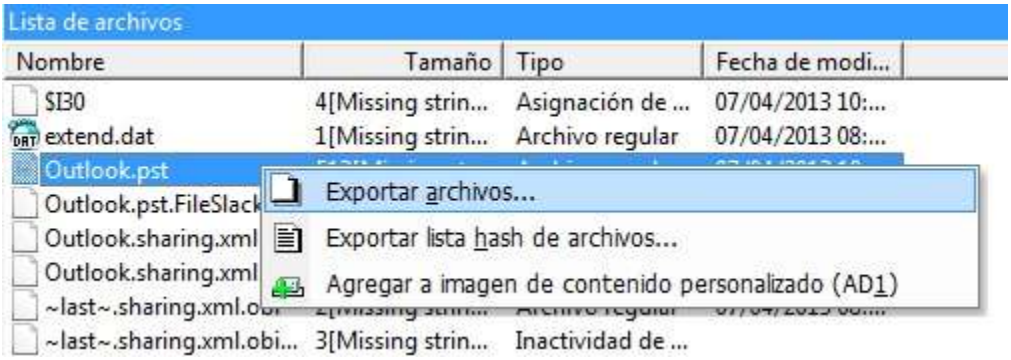


Figura 5.12 Extracción de registros de correo electrónico.

Una vez que se extrajo el archivo se obtuvo el hash MD5 del mismo (véase la figura 5.13), el cual fue documentado junto con otros datos relevantes del hallazgo en el formato INV-HED-01 (véase la Tabla 5.15).

Figura 5.13 Hash MD5 del registro de correo electrónico.

Tabla 5.15 Información sobre el hallazgo “Outlook.pst”.

Formato: ANA-HED-01	
Identificador de la imagen forense	IMGF-PC-009-DD01
Identificador del hallazgo	HED-01-PC-009-DD01
Nombre del hallazgo (archivo)	Outlook.pst
Ubicación del hallazgo (archivo)	C:\Documents and Settings\Consultorio\Configuración local\Datos de programa\Microsoft\Outlook\
Hash MD5 del hallazgo	220127f1f1b2bc8e268966a5fa152379
Descripción	Archivo que contiene el correo electrónico configurado para la cuenta de usuario “Consultorio” utilizada por la secretaria
Identificador del dispositivo de almacenamiento usado para copiar el hallazgo	ED-001

5.5.3.4. Análisis de los registros de correo.

Para acceder a los datos del archivo se utilizó la aplicación PSTViewer Pro 4, la cual permite consultar los datos almacenados en el archivo a través de una interfaz gráfica. En la siguiente imagen (véase la figura 5.14) puede observarse la interfaz gráfica de la aplicación listando el contenido de los correos enviados por la

cuenta “consul-med-ac@outlook.com” donde puede apreciarse que el día 7 de abril de 2013 a las 17:08 se envió un correo a la cuenta “farmacia-barata@outlook.com” con un archivo adjunto llamado “Datos Pacientes.xlsx”.

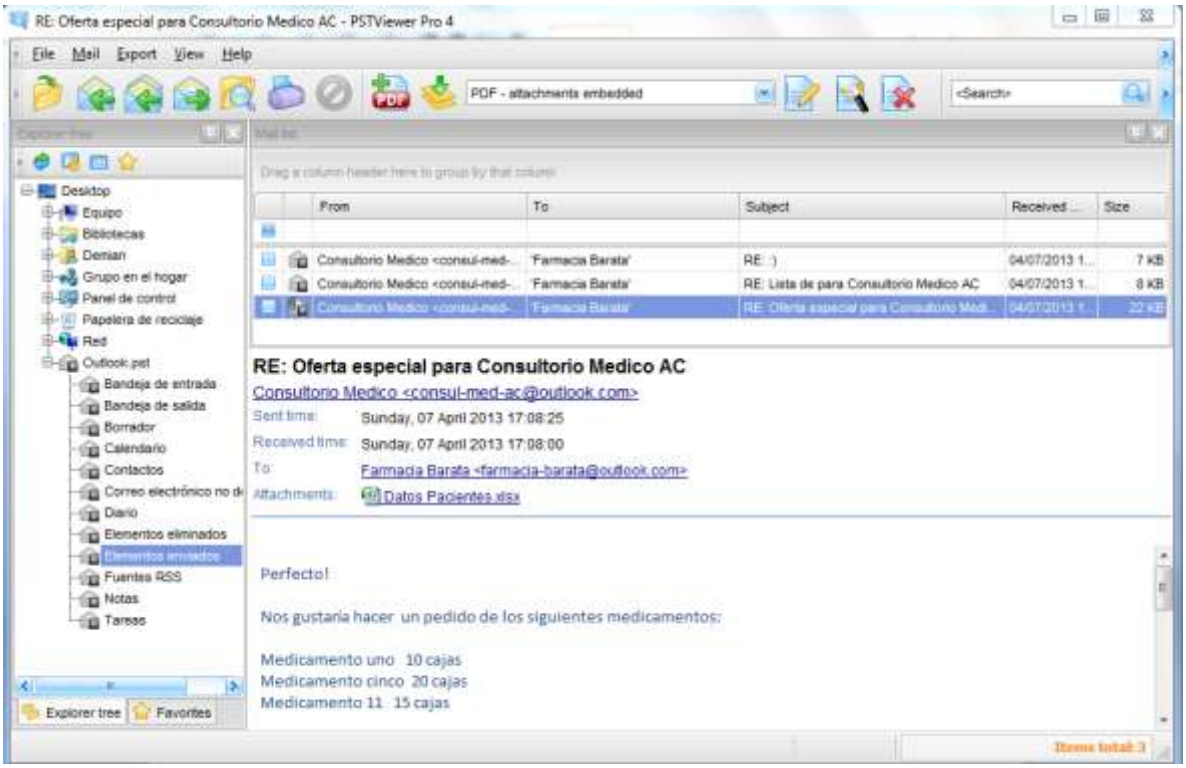
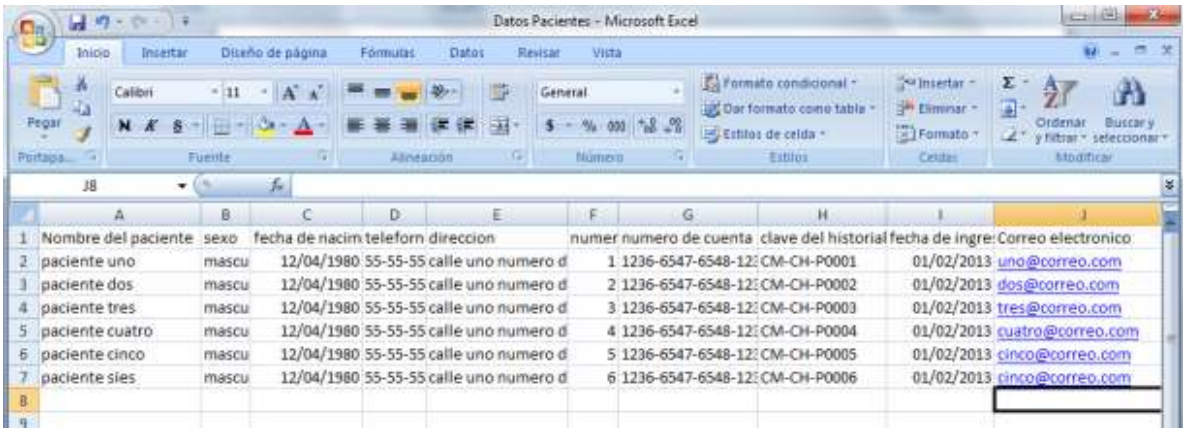


Figura 5.14 Correos enviados por “consul-med-ac@outlook.com”.

La herramienta PSTViewer Pro 4 permite recuperar el archivo que fue enviado como adjunto. La información de este hallazgo se encuentra documentada en el formato INV-HED-02 (véase la tabla 5.16), la figura 5.15 muestra el contenido del archivo “Datos Pacientes.xlsx”.



	A	B	C	D	E	F	G	H	I	J
1	Nombre del paciente	sexo	fecha de nacim	teleforn	direccion	numer	numero de cuenta	clave del historial	fecha de ingre	Correo electronico
2	paciente uno	mascu	12/04/1980	55-55-55	calle uno numero d	1	1236-6547-6548-12	CM-CH-P0001	01/02/2013	uno@correo.com
3	paciente dos	mascu	12/04/1980	55-55-55	calle uno numero d	2	1236-6547-6548-12	CM-CH-P0002	01/02/2013	dos@correo.com
4	paciente tres	mascu	12/04/1980	55-55-55	calle uno numero d	3	1236-6547-6548-12	CM-CH-P0003	01/02/2013	tres@correo.com
5	paciente cuatro	mascu	12/04/1980	55-55-55	calle uno numero d	4	1236-6547-6548-12	CM-CH-P0004	01/02/2013	cuatro@correo.com
6	paciente cinco	mascu	12/04/1980	55-55-55	calle uno numero d	5	1236-6547-6548-12	CM-CH-P0005	01/02/2013	cinco@correo.com
7	paciente sies	mascu	12/04/1980	55-55-55	calle uno numero d	6	1236-6547-6548-12	CM-CH-P0006	01/02/2013	cinco@correo.com
8										

Figura 5.15 Contenido del archivo “Datos Pacientes.xlsx”.

Tabla 5.15 Información sobre el hallazgo “Datos Pacientes.xlsx”.

Formato ANA-HED-02	
Identificador de la imagen forense	IMGF-PC-09-DD01
Identificador del hallazgo	ANA-HED-02
Nombre del hallazgo (archivo)	Datos Pacientes.xlsx
Ubicación del hallazgo (archivo)	C:\Documents and Settings\Consultorio\Configuración local\Datos de programa\Microsoft\Outlook\
Hash MD5 del hallazgo	220127f1f1b2bc8e268966a5fa152379
Descripción	Archivo de texto que contiene información confidencial enviado a una cuenta de correo ajena al Consultorio Médico AC.
Identificador del dispositivo de almacenamiento usado para copiar el hallazgo	ED-001

5.5.4. Recomendaciones.

- Establecer políticas de uso de los equipo de cómputo pertenecientes al consultorio.
- Implementar acuerdos de confidencialidad con todas las personas que manejen información de los pacientes y empleados.
- Redactar el Aviso de Privacidad según los lineamientos establecidos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
- Designar al responsable de atender las solicitudes de Acceso, Rectificación, Cancelación y Oposición al uso de datos personales según lo estipulado en la LFPDPPP.
- Establecer políticas para el uso, manejo y almacenamiento de los datos personales de pacientes y empleados del consultorio.
- Realizar campañas de concientización de seguridad de la información entre los empleados del consultorio.
- Cambiar el sistema operativo de las estaciones de trabajo que utilicen Windows XP por un sistema operativo que cuente con soporte para actualizaciones de seguridad a mediano y largo plazo.
- Implementar sistemas de cifrado para las estaciones de trabajo, por ejemplo, cifrado de Windows o aplicaciones comerciales como TrueCrypt.
- Utilizar herramientas de borrado seguro en las estaciones de trabajo.
- Instalar sistemas antivirus en las estaciones de trabajo del consultorio y definir políticas para la actualización frecuente de estos sistemas.
- Implementar políticas de contraseñas seguras para las estaciones de trabajo y cuentas de correo electrónico.

5.5.5. Conclusiones.

Después de analizar el sistema fue posible identificar que la fuga de información se llevó a cabo a través del servicio de correo electrónico. Se utilizó la cuenta "consul-med-ac@outlook.com" para enviar el archivo "datos Pacientes.xlsx", el cual contiene los datos personales y financieros de los pacientes del consultorio médico. La información fue enviada a la cuenta de correo "farmacia-barata@outlook.com" el día 7 de abril de 2013 a las 17:08.

De acuerdo a la información proporcionada al inicio de la investigación, la persona responsable de la cuenta de correo "consul-med-ac@outlook.com" es la secretaria Erika Lucio.

No hay evidencia del uso de algún otro mecanismo de extracción de información en el sistema. Tampoco existe evidencia de una posible intrusión no autorizada al sistema.

Capítulo 6

Implementación y resultados de la metodología en el Caso B.

El capítulo 6 presenta la aplicación de la metodología propuesta en este trabajo de investigación para la investigación de fuga de información provocada supuestamente por un empleado descontento, los detalles de este caso hipotético se precisan en el capítulo 4.

En esta investigación se emplean nuevas técnicas auxiliares que permiten obtener mayor información sobre el sistema afectado, estas técnicas son el análisis en vivo y el análisis básico de malware. Estas técnicas están contempladas en la metodología, donde se ofrece una guía general para su implementación.

En el transcurso de la investigación se identifica información relevante para determinar cómo ocurrió la fuga de información, mismos hallazgos que obligan a ampliar el alcance de la investigación contemplado inicialmente, demostrando la flexibilidad de la metodología propuesta.

Todas las actividades realizadas generan documentación, que puede ser consultada en las secciones de este capítulo o en el apartado de Anexos según corresponda. A continuación la aplicación de la metodología para la investigación de delitos informáticos en el Caso B.

6.1. Etapa de preparación.

De acuerdo con la metodología establecida en este trabajo de investigación, el primer paso a desarrollar es el proceso de preparación, este proceso se contempla la creación y configuración de la estación de trabajo a utilizarse en la investigación.

Para esta investigación se ha preparado una estación de trabajo que utiliza el sistema operativo Microsoft Windows 7 SP1 de 64 bits. Entre las aplicaciones

instaladas[30] se encuentra FTK Imager, los datos de la aplicación se documentan en el siguiente formato PREIN-APP-01 (véase la Tabla 6.1):

Tabla 6.1 Información sobre la aplicación FTK Imager.

Formato PREIN-APP-01	
Nombre de la aplicación	FTK Imager
Desarrollador	AccessData
Versión	3.1.3.
Hash MD5 del instalador	27868c05d6c0543fff9fe3f5b80d0e2e
Hash MD5 del ejecutable	f6d2c8f47461e589410a17c097c29385
Fuente de descarga	http://www.accessdata.com/support/product-downloads
Fecha de instalación	15/01/2013

Para alojar las imágenes forenses generadas, los hallazgos relevantes en la investigación, respaldo de archivos, entre otros, se preparan dispositivos de almacenamiento, esterilizándolos para eliminar cualquier dato que estuviera alojado en él. La documentación de este proceso se muestra en el siguiente formato PREIN-EDA-01 (véase la Tabla 6.2).

Tabla 6.2 Información sobre el dispositivo esterilizado.

Formato: PREIN-EDA-01	
Información del dispositivo	
Identificador del dispositivo para alojar evidencia	LAB-DDE-01
Marca/modelo	Adata/HD710
Número de serie	ADATA-4891943898

[30] Al ser una muestra del uso de la metodología, no se listan las características de todas las aplicaciones instaladas por cuestiones de practicidad. Se recomienda ampliamente que en una situación real se documente todas las aplicaciones usadas.

Capacidad	1.0 TB
Descripción	Disco duro externo con interfaz USB 3.0 listo para almacenar evidencia o artefactos forenses (volcados de memoria RAM, imágenes forenses)
Información sobre la esterilización	
Aplicación utilizada	Disk Wipe
MD5 de la aplicación	9b1e347cdaf1852cbd0538513c0056c4
Algoritmo utilizado	British HMG IS5
Número de pasadas	3
Fecha y hora de la esterilización	10/08/2013
Responsable de la esterilización	Demian García
Firma del responsable	ddd

6.2. Etapa de identificación.

Una vez terminado el proceso de preparación, el primer paso a seguir es conseguir la autorización correspondiente para iniciar la investigación. A continuación se presenta la carta de autorización:

Carta de autorización de Inicio de la investigación
Fecha: 21 de agosto de 2013 Por medio de la presente se concede autorización expresa por parte del representante de la empresa **Seguridad y Vigilancia iW**, **Ing. Julieta Guerrero**, al equipo de investigación liderado por, **Demian García**, para iniciar la investigación en cómputo forense con identificador: **Caso B-201306-SVIW**. La investigación contempla la revisión de la estación de trabajo **Dell-DSK1200** con número de serie: **5478941176**. Con disco duro marca: **SeaGate** modelo: **SG-3951c** con capacidad de: **80GB** y número de serie: **3259234132-ERC-123**. Así mismo, el representante de la empresa se compromete a apoyar y proveer todas las facilidades necesarias al equipo de investigación para que éste pueda llevar cabo la tarea sin complicaciones. _____ _____ Firma del representante de la empresa Firma del líder de la investigación.

Una vez que la misiva ha sido firmada por las partes correspondientes, se hace entrega de la carta de confidencialidad:

Carta de confidencialidad.

Fecha: 21 de agosto de 2013

Por medio de la presente, el equipo de investigación liderado por **Demian García** se compromete a respetar la privacidad de la información, relacionada con la empresa **Seguridad y Vigilancia iW**, al considerarla como estrictamente confidencial y de uso exclusivo a los procesos relacionados con la investigación en cómputo forense **Caso B-201306-SVIW** , por lo cual, el equipo de investigación se abstendrá de divulgarla, publicarla, distribuirla a terceros, utilizarla en provecho propio, y de conservar copias, respaldos totales o parciales, ya sean electrónicos o físicos, sin la autorización del representante de la empresa.

_____	_____
Nombre y firma del líder de la investigación	Nombre y firma del representante de la empresa

Cuando las cartas han sido firmadas se documenta la información del personal que conforma al equipo de investigación, esta información se recopila en el formato IDE-EIF-01 (véase la Tabla 6.3).

Tabla 6.3 Información de los integrantes del equipo asignado a la investigación.

Formato: IDE-IEF-01	
Identificador del investigador	EIF-DRGV-19981101
Nombre	Demian García
Rol en la investigación	Líder de la investigación
Firma	
Identificación con fotografía	

En este punto, después de que las cartas han sido firmadas, es posible iniciar la investigación, el primer paso es recopilar información relacionada a la empresa, al incidente de seguridad, la atención del incidente y otros temas que resulten de interés. Toda la información recopilada es almacenada en diferentes formatos, lo que facilita futuras consultas.

En el formato IDE-INV-*Caso B-201306-VSIW* (véase la Tabla 6.4) se recopila información general sobre la investigación para iniciar el expediente correspondiente, incluye datos como el identificador de la investigación, el cual es único y engloba todos los procedimientos desarrollados en la investigación, datos generales de la empresa afectada y fechas de inicio.

Tabla 6.4 Información general acerca de la investigación.

Formato: IDE-INV-Caso B-201306-VSIW	
Identificador de la investigación	Caso B-201306-VSIW
Tipo de incidente	Fuga de información confidencial. Se pretende identificar al responsable.
Activo afectado	Archivos de texto confidenciales que contienen propuestas para la realización de diferentes proyectos.
Fecha de inicio	21 de agosto de 2013

Investigador asignado	Demian García
Datos generales de la empresa afectada	
Nombre	Vigilancia y Seguridad IW
Giro	Instalación y mantenimiento de sistemas de vigilancia
Dirección	Calle Bolívar Col. Portales, Delegación Milpa alta, Distrito Federal, México.
Director General	Ing. Julieta Guerrero
Contacto	jguerrero@gmail.com tel. 55-123-445 cel. 044-55-532-445-11

El día 21 de agosto de 2013 la Ing. Julieta Guerrero ha solicitado una investigación basada en cómputo forense para identificar al responsable de la fuga de información confidencial relacionada a propuestas para el desarrollo de diferentes proyectos relacionados con sistemas de seguridad.

La solicitud de esta investigación es generada por la sospecha de que un empleado filtre información confidencial a una empresa competidora de Vigilancia y Seguridad IW.

La información confidencial es condensada en documentos de texto que contienen especificaciones técnicas y documentales sobre el diseño de sistemas de seguridad. Estos documentos son generados por el empleado Salvador Pedrosa en su estación de trabajo.

La metodología establece el uso de un cuestionario con preguntas dirigidas al personal involucrado en el incidente. El formato IDE-ISE-01 documenta los datos de las personas entrevistadas (véase la Tabla 6.5).

Tabla 6.5 Información de los empleados de la empresa afectada.

Formato: IDE-ISE-01	
Empleado 1	
Nombre	Julieta Guerrero
Puesto	Directora de SVIW
Descripción de actividades	Diseño de sistemas de vigilancia y desarrollo de cotizaciones para diferentes proyectos.
Firma	
Identificación con fotografía	
Todas personas mencionadas en este documento al momento de firmarlo aceptan que la información aquí recabada es verídica.	

A continuación se presenta el cuestionario aplicado en la entrevista:

a) ¿Qué activo informático se vio afectado en el incidente de seguridad?
b) ¿Dónde se encuentra alojado dicho activo (ubicación física del dispositivo)?
c) ¿Quién es el responsable del equipo en el que el activo se encuentra alojado?
d) ¿Quién tiene acceso a tal equipo?
e) ¿El equipo se encuentra conectado a una red?, de ser así ¿Cuál es la información relacionada con la red?
d) Al inicio de la investigación, ¿El equipo se encuentra encendido o apagado?

El resultado del proceso de entrevista señala que los activos afectados incluyen varios documentos de texto, imágenes y planos. Los archivos son manejados principalmente por el Ing. Salvador Pedrosa y en menor medida por Julieta Guerrero. Los documentos principales son generados por Ing. Salvador Pedrosa. Ningún otro empleado maneja este tipo de información.

El resultado de la entrevista se documenta en los formatos IDE-AIT-01 (véase la Tabla 6.6), IDE-HW-01 (véase la Tabla 6.7), y IDE-RED-01 (véase la Tabla 6.8).

Tabla 6.6 Información relacionada al activo de información afectado.

Formato: IDE-AIT-01	
Identificador del activo	AIT-01
Tipo de activo	Documentos de texto.
Extensión	Posiblemente .doc, .docx o .pdf
Software asociado	Microsoft Word, Adobe Reader
Descripción	Propuestas de diseño y cotizaciones para desarrollo de proyectos relacionados a seguridad y vigilancia.
Usuarios con acceso al archivo	Salvador Pedrosa
Equipo en el que está ubicado	PC-01
Responsable del activo	Salvador Pedrosa

Tabla 6.7 Información sobre el equipo que almacena el activo afectado.

Formato: IDE-HWD-001	
Tipo de dispositivo	Estación de Trabajo (PC)
Identificador del dispositivo	PC-01
Marca/Modelo	Dell/DSK1200
Número de Serie	5478941176
Características Generales	Computadora de escritorio marca Dell, gabinete color gris.
¿El equipo se encuentra encendido?	Equipo encendido y con sesión iniciada.
Disco Duro asociado al equipo(1)	
Identificador del disco	PC-01-DD01

duro	
Marca	SeaGate
Modelo	SG-3951c
Número de serie	3259234132-ERC-123
Capacidad de almacenamiento	80 GB
Tipo de Interfaz	IDE
Ubicación del equipo	
Área a la que pertenece	Diseño y planeación
Empresa/Organización	Seguridad y Vigilancia iw
Dirección	Calle 84 #131 Col. Nápoles. DF
Información adicional	N/A
Responsable del equipo	
Nombre del responsable	Ing. Salvador Pedrosa
Nombre de usuario	Administrador
Puesto	Consultor
Correo electrónico	spedrosa@mail.com
Teléfono	551199327750
Descripción de actividades	Diseño y presentación de propuestas para realización de proyectos, generación de cotizaciones
Conectividad	
Red a la que se conecta el equipo	Red SVIW
Tipo de conexión	Alámbrica, cable Ethernet
Software	
Sistema operativo	Windows XP SP2

Tabla 6.8 Información sobre la red a la que está conectado el equipo.

Formato: IDE-RED-01	
Tipo de red	LAN
Tipo de conexión	Alámbrica, cable Ethernet
Topología de red	Estrella
Número de equipos conectados	2
ISP	UNINET
Administrador de la red	
Nombre	--
Correo	--
Tel	--
Comentario	No hay personal asignado a la administración de la red

6.3. Análisis en vivo.

Debido a que el equipo se encuentra encendido y con una sesión iniciada es imperativo que inicie el proceso de análisis en vivo y la preservación de información volátil.

6.3.1. Procesos en ejecución.

El equipo a investigar utiliza un sistema operativo de la familia Microsoft Windows, específicamente la versión XP. Por tal motivo es posible obtener información de los procesos en ejecución con la ayuda de la herramienta **Process Explorer**, desarrollada por **Sysinternals**, una subdivisión de Microsoft. Esta aplicación portable muestra información acerca de cada proceso en ejecución así como información sobre la compañía que desarrolla el programa y una descripción de

cada proceso. La siguiente figura (véase la figura 6.1) muestra los procesos en ejecución en el equipo investigado.

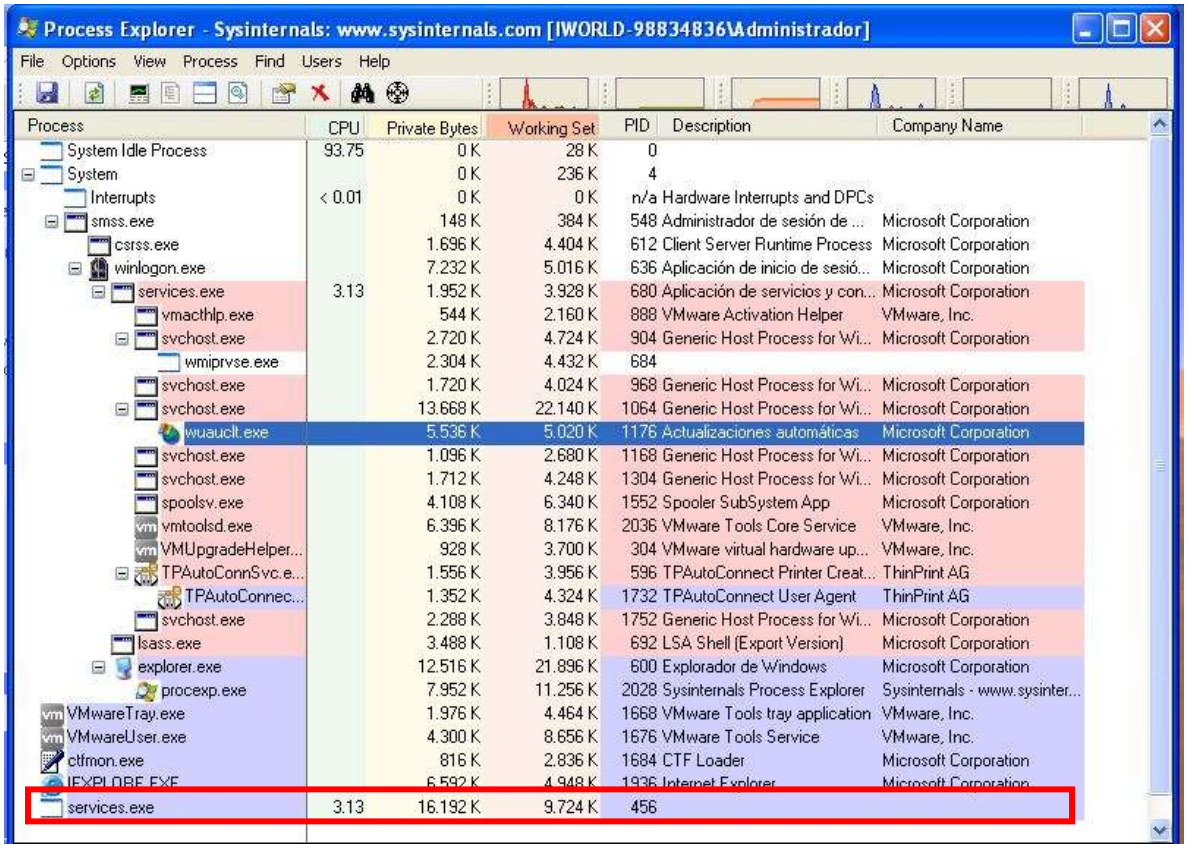


Figura 6.1 Procesos listados por Process Explorer.

En la figura 6.1 puede apreciarse un proceso que no posee descripción alguna ni un nombre de la compañía que lo desarrolla, la ausencia de estos datos apunta a un proceso sospechoso. El proceso en cuestión tiene por nombre “services.exe” y como PID (Identificador de proceso por sus siglas en inglés) 456. Una vez identificado el proceso sospecho se debe tomar nota del nombre y del PID correspondiente.

El siguiente paso en la recolección de información volátil es listar las conexiones establecidas en el equipo.

6.3.2. Conexiones establecidas.

Para conocer cuáles son las conexiones establecidas en el equipo sospechoso se puede utilizar la herramienta **TCPView,** también desarrollada por Sysinternals. Esta herramienta lista las conexiones establecidas mostrando direcciones locales y puerto local utilizado, direcciones remotas y puertos remotos, protocolo utilizado y el proceso que está utilizando dicha conexión. La siguiente imagen (véase la figura 6.2) muestra las conexiones establecidas en el equipo sospechoso.

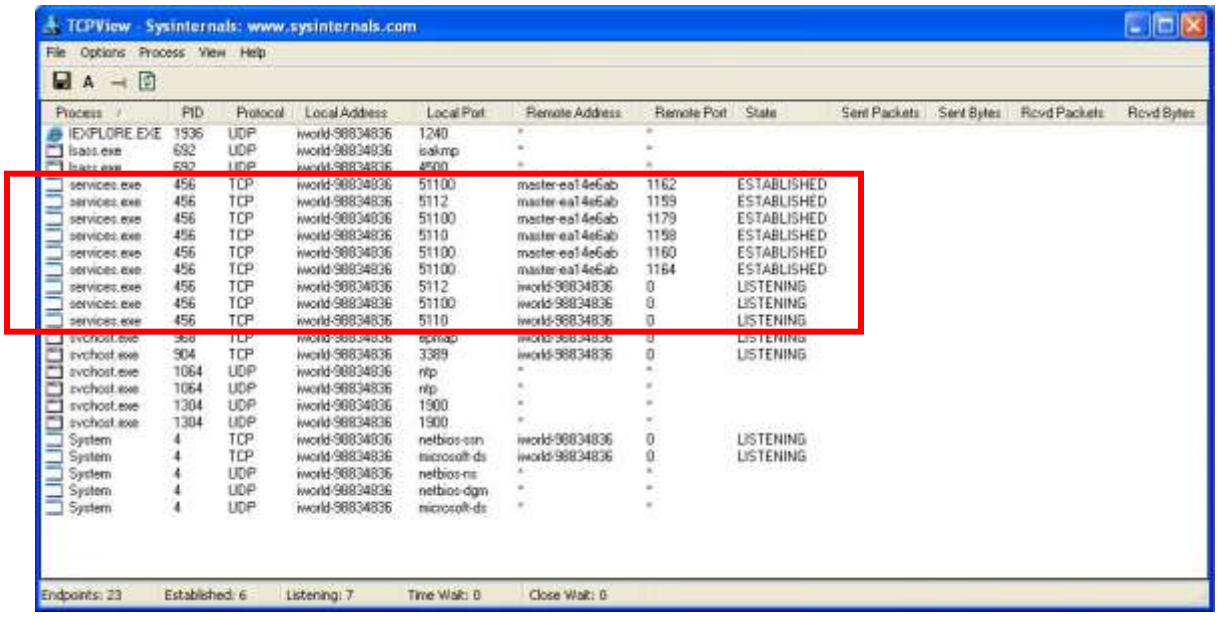


Figura 6.2 Conexiones establecidas en el equipo sospechoso.

Es posible apreciar que el proceso "*services.exe*" con PID 456 tiene varias conexiones establecidas con un equipo desconocido que tiene asociado el nombre "Master-ea14e6ab". También se puede apreciar que el proceso sospechoso ha puesto tres puertos a la escucha de nuevas conexiones entrantes.

El comportamiento mostrado por este programa es bastante inusual, por lo que debe investigarse. De acuerdo a la metodología es necesario compilar la información recolectada al momento y generar un perfil del proceso sospechoso, la información relacionada al proceso se muestra en la tabla 6.9.

Tabla 6.9 Información de las conexiones de red del proceso sospechoso.

Identificador del hallazgo			ANA-HED-01	
Identificador del dispositivo origen			PC-01	
Descripción			Información sobre conexiones de red relacionadas con un proceso sospechoso, obtenidas mediante la herramienta TCPView.	
Nombre del proceso			Services.exe	
PID			456	
Puerto local	Host remoto	Puerto remoto	Protocolo	Estado de la conexión
5112	Master-ea14e6ab	1159	TCP	Establecida
51100	Master-ea14e6ab	1162	TCP	Establecida
51100	Master-ea14e6ab	1179	TCP	Establecida
5110	Master-ea14e6ab	1158	TCP	Establecida
51100	Master-ea14e6ab	1160	TCP	Establecida
51100	Master-ea14e6ab	1164	TCP	Establecida
5112	localhost	0	TCP	A la escucha
51100	localhost	0	TCP	A la escucha
5110	localhost	0	TCP	A la escucha

A través de la herramienta Process Explorer es posible visualizar las propiedades del proceso sospechoso, entre los valores que pueden visualizarse se encuentra la ruta donde está alojado el programa ejecutable, los hilos que utiliza, las

conexiones **TCP/IP**, datos sobre el desempeño del proceso y algunas instrucciones utilizadas por el proceso. La siguiente imagen (véase la figura 6.3) corresponde a las propiedades del proceso “services.exe”.

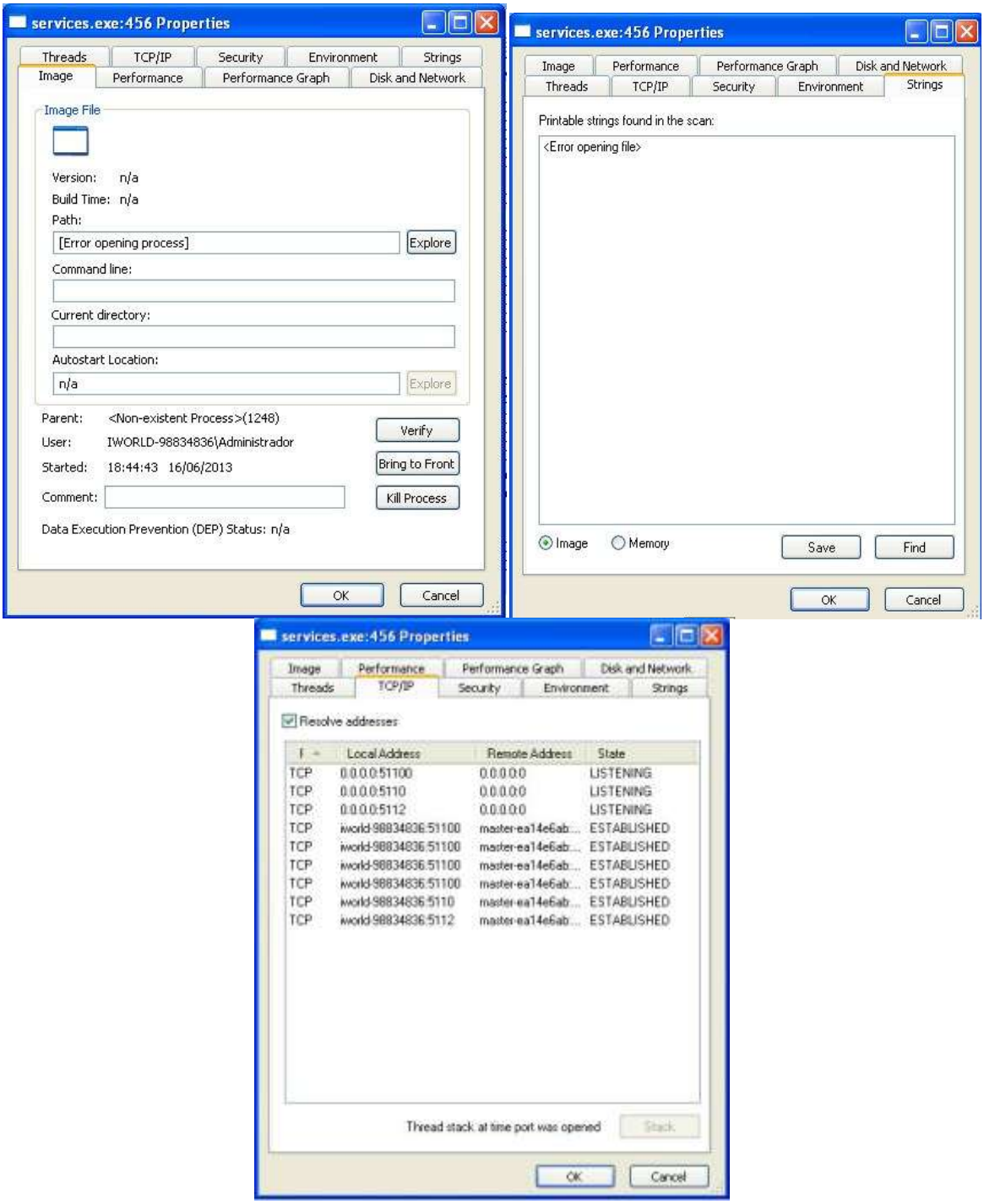


Figura 6.3 Propiedades del proceso services.exe

Se aprecia que ocurrió un error al abrir el proceso y no es posible conocer la ruta en la que está alojado el archivo ejecutable, tampoco es posible ver el contenido del ejecutable en el apartado "*Strings*" pero se puede verificar que el proceso mantiene conexiones establecidas con el host "master" y se encuentra a la espera de nuevas conexiones. El uso de dichas conexiones es un punto que se debe tomar en cuenta ya que se está investigando una fuga de información confidencial y una conexión con un host desconocido puede ser un camino para las filtraciones de información.

Sin embargo, debido a las características de este programa sospechoso y a las limitaciones de las herramientas utilizadas hasta ahora es necesario abordar el problema desde otra perspectiva. Para continuar con la investigación se realiza un volcado de memoria RAM.

6.3.3. Volcado y análisis de memoria RAM.

El proceso de volcado de memoria pretende representar toda la información alojada de manera volátil en la memoria RAM en un archivo que permita su estudio de manera independiente al sistema que está siendo investigado. Una forma de ver este proceso es imaginar que se toma una fotografía de los datos que procesa la memoria RAM en un determinado momento.

Para realizar este análisis se utilizan dos herramientas, **DumpIt** para generar un archivo con el volcado de memoria y **Volatility** para analizar el archivo generado.

La siguiente imagen (véase la figura 6.4) muestra la interfaz de DumpIt, al ejecutar la herramienta se muestra una consola que informa el tamaño del espacio asignado a la memoria RAM, el destino del archivo que se va a generar, el cual es la misma ubicación donde se encuentra la herramienta, y espera la confirmación del usuario para iniciar el proceso de volcado. La ventaja de esta herramienta es que no requiere de instalación y puede ser ejecutada desde una memoria flash,

estas características reducen la cantidad de datos en memoria sobrescritos por la herramienta.

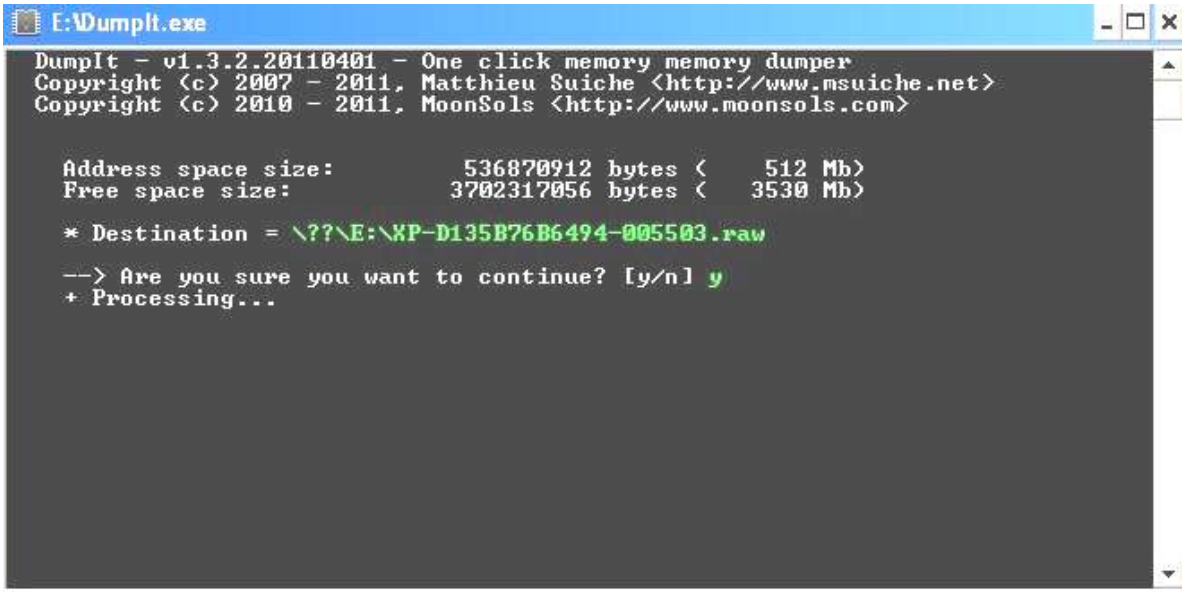


Figura 6.4 Interfaz de DumpIt para generar el volcado de memoria.

Una vez terminado el proceso de generación del archivo con el volcado de memoria se debe agregar el artefacto a la cadena de custodia. Por tal motivo inicia el proceso de cadena de custodia de acuerdo a la metodología propuesta. En la Tabla 6.10 se documenta información importante sobre el proceso de cadena de custodia

Tabla 6.10 Información general relacionada con el proceso de la cadena de custodia

Formato: PRE-CC-01	
Identificador de la cadena de custodia	CC-01
Identificador de la investigación	*Caso B-201306-VSIW*
Identificador del custodio asignado	ICF-DGV-201306
Descripción de los dispositivos	Dispositivo 1: Archivo de volcado del contenido de memoria RAM del sistema utilizado por Salvador Pedrosa. Dispositivo 2: Disco duro de 80 GB que

	contiene sistema operativo y datos del usuario Salvador Pedrosa. Dispositivo 3: Disco duro para almacenar evidencia e imágenes forenses.
Datos del dispositivo 1	
Identificador del dispositivo	MDUMP-PC-01
Bitácora asociada	LOG-CC-01
Fecha y hora de inserción a la cadena	21/08/2013 16:00hrs
Datos del dispositivo 2	
Identificador del dispositivo	PC-01-D01
Bitácora asociada	LOG-CC-02
Fecha y hora de inserción a la cadena	21/08/2013 16:00hrs
Datos del dispositivo 3	
Identificador del dispositivo	LAB-DDE-01
Bitácora asignada	LOG-CC-03
Fecha y hora de inserción a la cadena	21/08/2013 16:00hrs

La generación de un archivo de volcado de memoria debe ser documentado, contemplando los puntos mostrados en el formato PRE-GVM.01 (véase la tabla 6.11), cabe destacar que el archivo resultante es contemplado dentro de la cadena de custodia.

Tabla 6.11 Información referente a la generación del volcado de memoria.

Formato: PRE-GVM-01	
Identificadores	
Identificador del volcado de memoria	MDUMP-PC-01-RAM01
Identificador del dispositivo origen	PC-01-RAM01
Identificador de la cadena de custodia a la que pertenece el dispositivo	CC-01
Identificador del dispositivo donde se	LAB-DDE-01

aloja el volcado de memoria	
Información de la generación de la imagen	
Herramienta usada	DumpIt
MD5 de la herramienta	84f0feb07beae896d471f45527d781b0
Identificador del dispositivo donde se aloja la imagen	ED-001
Nombre del archivo generado	memDump.bin
MD5 de la imagen generada	ef6a7ab2afb99dfdb3218f9d35998130
Formato de la imagen	.bin
Tamaño de la imagen	512MB
Responsable de la generación del a imagen	Demian García
Firma del responsable	
Hora y fecha de la generación	21 agosto 2013, 16:10hrs
Identificado de la bitácora de hashes	HASH- PC-001-RAM001

La herramienta Volatility es un conjunto de programas, conocidos como *plugins*, de código abierto diseñados para interpretar el contenido de archivos sin formato, también conocidos como **archivos *raw***, que son el resultado de un volcado de memoria. La herramienta se utiliza a través de una consola mediante diferentes comandos, se puede especificar el tipo de sistema al que pertenecían los datos volcados de la RAM para que los programas sepan qué estructuras de datos buscar.

Esta especificación se hace mediante perfiles establecidos para cada tipo de sistema operativo, versión y arquitectura usada. En este caso el perfil corresponde a un equipo de 32 bits con sistema operativo Windows XP con Service Pack 2, es decir “--profile=WinXPSP2x86”.

La siguiente imagen (véase la figura 6.5) muestra el listado de procesos alojados en memoria:

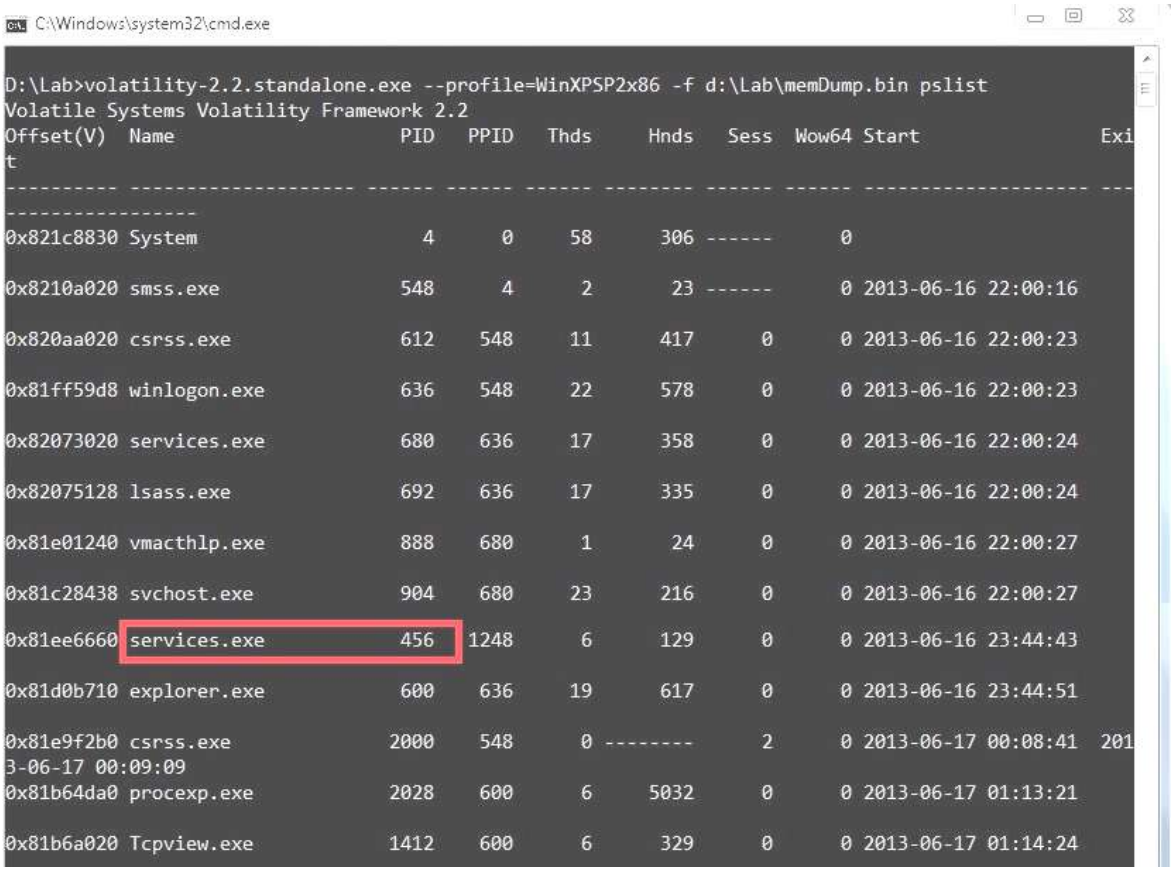


Figura 6.5Procesos alojados en memoria listados por Volatility.

El proceso sospechoso también es detectado por esta herramienta. Cuando se ejecuta, el proceso es cargado en memoria, el volcado de memoria permite recuperar los datos alojados en ella, de tal modo que si Volatility identifica que el proceso está en la imagen obtenida es posible reconstruir en un archivo ejecutable el conjunto de instrucciones utilizadas por el proceso sospechoso.

Esta operación puede ejecutarse con el comando "*procexedump -p 456*" donde la opción –p indica el PID correspondiente al proceso que se desea obtener. La siguiente imagen (véase la figura 6.6) muestra el resultado de la ejecución de este comando.

0p

```
D:\Lab>volatility-2.2.standalone.exe --profile=WinXPSP2x86 -f d:\Lab\memDump.bin procexedump -p 456
--dump-dir=.
Volatile Systems Volatility Framework 2.2
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81ee6660 0x00400000 services.exe         OK: executable.456.exe
```

Figura 6.6 Procesos alojados en memoria listados por Volatility.

La opción "*—dump-dir=.*" Indica el directorio donde se guarda el archivo generado, en este caso es el directorio actual. La información relacionada a este hallazgo se documenta en la tabla 6.12.

Tabla 6.12 Información sobre el proceso sospechoso encontrado en memoria.

Identificador del hallazgo	ANA-HED-02
Identificador del dispositivo origen	PC-01
Identificador del artefacto forense origen	MDUMP-PC-01
Identificador de la cadena de custodia	CC-01
Identificador del dispositivo que aloja el hallazgo	LAB-DDE-01
Descripción	Archivo ejecutable generado por lsa instrucciones cargadas en memoria ram por el proceso services.exe con PID 456.
Proceso	services.exe
PID	456
Ejecutable generado	executable.456.exe
Hash MD5	770f707aacdf543d50436f7db96f6dda

Cuando se obtiene el archivo ejecutable se analiza su contenido a través de la aplicación "strings" de SysInternals[31], esta aplicación interpreta las cadenas de

[31] http://technet.microsoft.com/en-us/sysinternals/bb897439

texto embebidas en el ejecutable y las imprime de una forma legible. La figura 6.7 muestra algunas cadenas que llaman la atención.

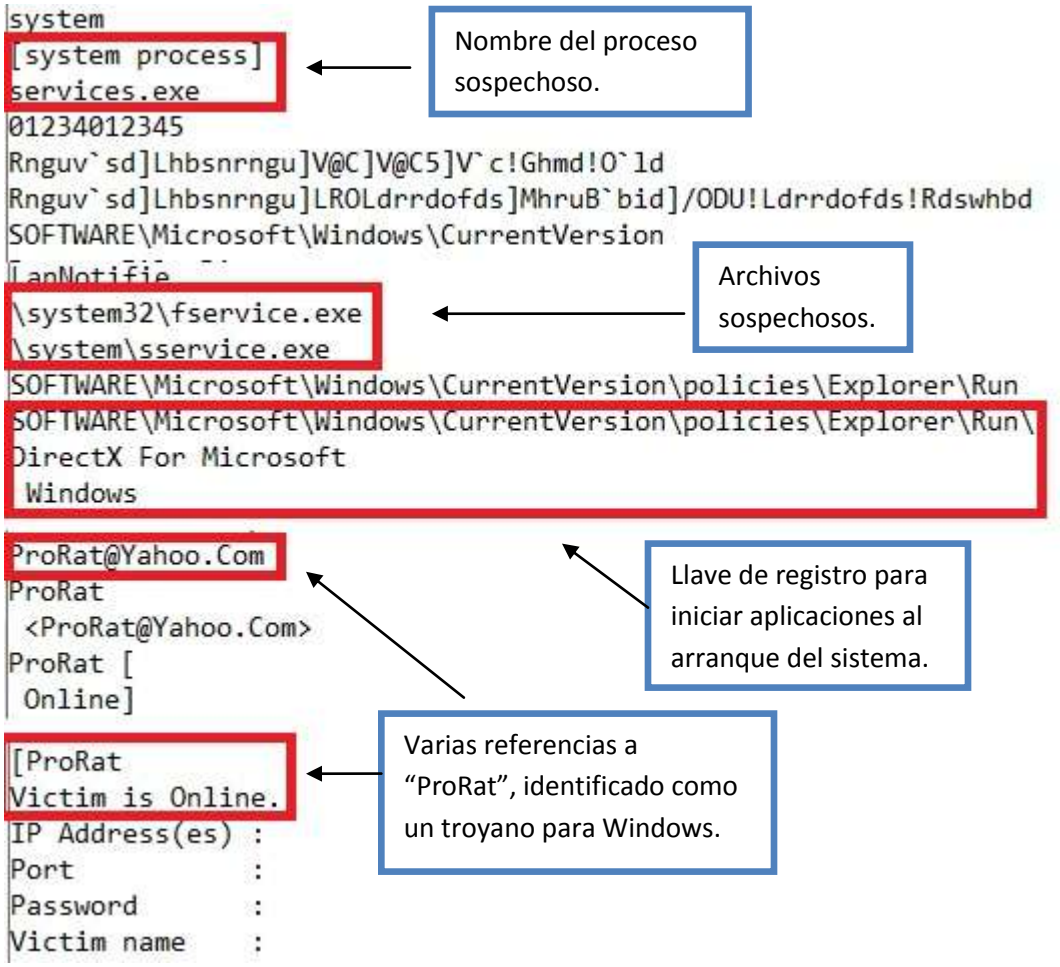


Figura 6.7 Cadenas sospechosas del archivo "executable.456.exe".

Las cadenas presentadas en la figura anterior forman parte de las instrucciones ejecutadas por el proceso "services.exe", mismas que sugieren que se trata de un proceso malicioso. Es posible utilizar el sitio www.virustotal.com para analizar el archivo generado y comprobar si es identificado como malicioso (véase la figura 6.8).

Figura 6.8 Análisis del archivo creado en Virus Total.

Este sitio contiene una base de datos con firmas de malware conocido generadas por decenas de firmas antivirus. El análisis se realiza al obtener varias firmas hash, **SHA1**, MD5, entre otras, y comparar esos valores con los almacenados en la base de datos. La siguiente imagen (véase la figura 6.9) muestra el resultado del análisis.

Figura 6.9 Resultado del análisis del ejecutable generado con Volatility.

Un gran número de firmas antivirus identifican el archivo como malicioso, y varias lo catalogan como **troyano**. Es probable que este archivo esté involucrado en la fuga de información pero es necesario obtener más información.

Continuando con el análisis del volcado de memoria, se listan las aplicaciones más usadas por el usuario a través del módulo "*usserassist*" de Volatility, el sistema operativo cuenta con un registro del número de veces que un usuario ejecuta cada aplicación y guarda el dato en una llave para cada usuario.

Éste módulo permite listar todas las aplicaciones y el número de veces que ha sido ejecutada cada una, así como la ubicación de la aplicación y la fecha de la última ejecución. La siguiente tabla (véase la tabla 6.13) recopila algunas aplicaciones ejecutadas por el usuario.

Tabla 6.13 Algunas aplicaciones ejecutadas por la cuenta de usuario "Administrador".

REG_BINARY UEME_RUNPATH: C:\Documents and Settings\Administrador\Mis documentos\Descargas\descuentoCam.exe : ID: 2 Count: 1 Last updated: 2013-07-17 23:18:18 0x00000000 02 00 00 00 06 00 00 00 a0 b6 22 79 eb 6a ce 01 ....."y.j.
REG_BINARY UEME_RUNPATH:C:\Documents and Settings\Administrador\Escritorio\ProcessExplorer\procexp.exe : ID: 2 Count: 1 Last updated: 2013-08-21 16:03:21 0x00000000 02 00 00 00 06 00 00 00 d0 cb 9b db f7 6a ce 01 .....j..
REG_BINARY UEME_RUNPATH:C:\Documents and Settings\Administrador\Escritorio\TCPView\Tcpview.exe : ID: 2 Count: 1 Last updated: 2013-08-21 16:04:24 0x00000000 02 00 00 00 06 00 00 00 c0 7e 64 01 f8 6a ce 01 .....~d..j..

Una aplicación que llama la atención es "*descuentoCam.exe*" debido a que el nombre es peculiar y no se relaciona a una aplicación comercial. Al listar el

contenido del directorio "C:\Documents and Settings\Administrador\Mis documentos\Descargas\" no es posible apreciar dicha aplicación, sin embargo existe un archivo comprimido y una imagen que utilizan el mismo nombre (véase la figura 6.10).

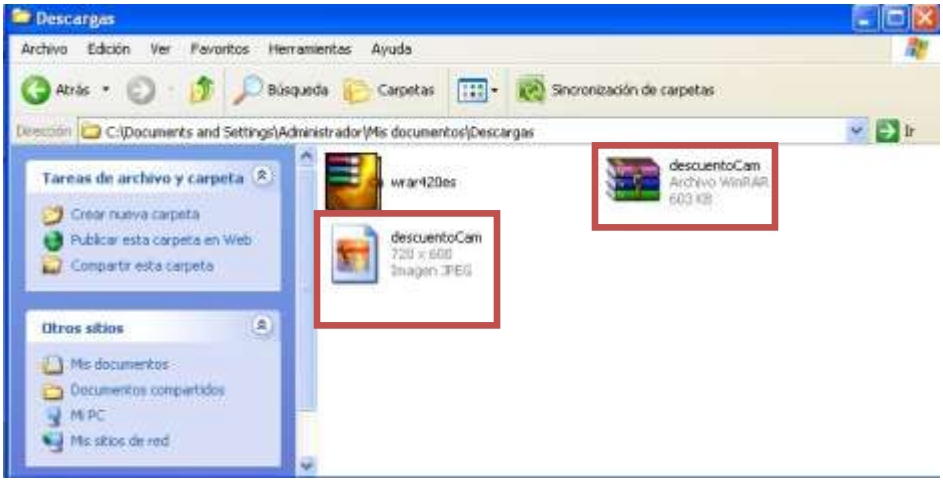


Figura 6.10 Contenido del directorio de Descargas.

Es posible hacer una copia del archivo comprimido y revisar su contenido en la estación de investigación, los datos de este archivo se documentan en la tabla 6.14.

Tabla 6.14 Datos del archivo comprimido.

Identificador de hallazgo	ANA-HED-03
Identificador del dispositivo origen	PC-01-D01
Identificador del dispositivo que aloja la evidencia	LAB-DDE-01
Descripción	Archivo comprimido sospecho, posiblemente relacionado a una aplicación maliciosa
Nombre	descuentosCam.rar
Ubicación	C:\Documents and Settings\Administrador\ Mis documentos\Descargas\
Hash MD5	070f6618a9500eef793984283621feaa

Al descomprimir el archivo "descuentoCam.rar" se identifica la aplicación "descuentoCam.exe" (véase la figura 6.11). Para identificar si se trata de una aplicación inofensiva se utiliza el servicio de Virus Total para analizar el archivo. El resultado del análisis de muestra en la siguiente figura (véase la figura 6.12).

Figura 6.11 Contenido del archivo comprimido "descuentoCam.rar".

Figura 6.12 Resultado del análisis de aplicación sospechosa.

El análisis indica que el archivo es malicioso y ha sido identificado como un troyano de tipo ProRAT, donde las siglas RAT significan *Remote Administration Tool* o *Remote Access Trojan*. Este tipo de malware permite el acceso al equipo

infectado de manera remota y ofrece control total del sistema infectado al intruso, quien puede controlar la cámara web, registrar todo lo que se teclee en el equipo, realizar todo tipo de modificaciones sobre archivos, cargar archivos de manera remota o descargar archivos alojados en el equipo infectado.

Debido a las características maliciosas de este archivo es necesario documentarlo como hallazgo ya que probablemente esté relacionado con la fuga de información. Su documentación se muestra en la tabla 6.15.

Tabla 6.15 Información sobre el hallazgo “descuentosCam.exe”.

Identificador del hallazgo	ANA-HED-04
Identificador del archivo	HED-04-001
Nombre del archivo	descuentosCam.exe
Hash MD5	1072f5cee0640caaefa48843eda6614c
Ubicación del archivo	C:\Documents and Settings\Administrador\ Mis documentos\Descargas\
Identificador del dispositivo origen	PC-01-D01
Identificador del artefacto forense origen	IMGF-PC-01-DD01
Identificador del dispositivo usado para almacenar la evidencia	LAB-DDE-01

En este punto se han identificado dos aplicaciones maliciosas, “services.exe” y “descuentosCam.exe”. “services.exe” es una aplicación que se encuentra en ejecución y a través de un volcado de memoria se obtuvieron algunas de las instrucciones que ejecuta, en ellas se hace mención del nombre “ProRAT” en las cadenas embebidas en el ejecutable, esta aplicación establece conexiones con un equipo remoto a través de diferentes puertos. La segunda aplicación maliciosa, “descuentosCam.exe”, se identificó en un archivo comprimido en el mismo

directorio donde se ejecutó una aplicación con el mismo nombre, al analizar la aplicación utilizando el servicio de Virus Total se ha determinado que se trata de un troyano.

La información obtenida hasta el momento, las respuestas de los empleados en la entrevista y los datos recolectados durante el análisis en vivo del sistema, permiten plantear una primera hipótesis para abordar el caso.

Hipótesis:
La fuga de información se presenta debido a una aplicación maliciosa que permite el acceso al equipo de manera remota y no autorizada. Este tipo de acceso a través de malware facilita el robo de cualquier archivo alojado en el sistema. Es probable que la aplicación “descuentosCam.exe” sea la responsable de generar el proceso “services.exe” que permite las conexiones al equipo.

Es necesario demostrar que ambas aplicaciones están relacionadas entre sí para apoyar la hipótesis planteada. Para probar la relación entre ambas aplicaciones es posible acudir a la metodología presentada en este trabajo y utilizar la guía de análisis básico de malware esperando que su aplicación genere resultados que contribuyan a la investigación.

6.4. Análisis básico de malware.

El objetivo de este análisis es determinar una relación entre las aplicaciones maliciosas detectadas hasta este momento. La hipótesis plantea que la aplicación “descuentosCam.exe” es responsable de generar el proceso “services.exe”.

Para identificar esa relación, la metodología propone un análisis en cinco pasos.

6.4.1. Paso 1. Creación de un ambiente virtual.

Para este paso se crea una máquina virtual con el mismo sistema operativo utilizado en el equipo investigado, en este caso es Windows XP SP2 con una arquitectura de 32 bits.

6.4.2. Paso 2. Documentación del estado del sistema recién instalado.

Para este análisis en particular se documentan los procesos en ejecución, las conexiones de red y las aplicaciones que se ejecutan al iniciar el sistema. Las herramientas utilizadas para esta recolección de información son ProcessExplorer y TCPview, mismas que fueron utilizadas en el análisis en vivo de esta investigación. Para listar las aplicaciones que son ejecutadas al iniciar el sistema se utiliza **Autoruns**, una aplicación más de Sysinternals.

En la figura 6.13 se muestran los procesos en ejecución una vez que ha terminado la instalación del sistema operativo.

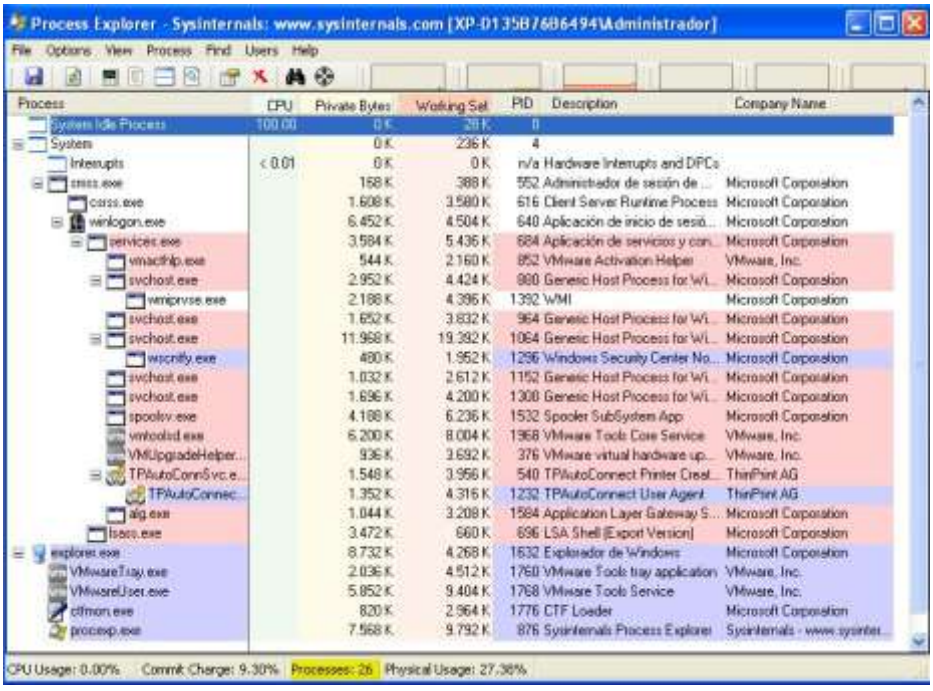


Figura 6.13 Procesos en ejecución después de la instalación del sistema operativo.

La herramienta señala un total de 26 procesos en ejecución, entre los cuales pueden observarse procesos del software utilizado para la **virtualización**, el proceso de la herramienta ProcessExplorer y procesos del sistema operativo.

A continuación se documentan las conexiones de red en el sistema recién instalado. (Véase la figura 6.14)

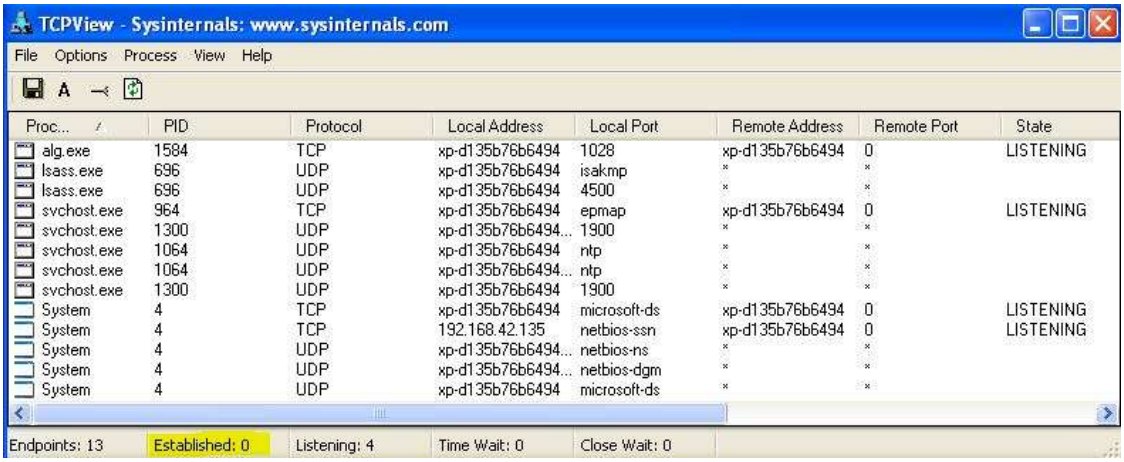


Figura 6.14 Conexiones de red en el sistema recién instalado.

La herramienta TCPView reporta que no hay conexiones establecidas y que existen cuatro puertos a la escucha de conexiones entrantes, todas producto del sistema operativo.

Al ejecutar la aplicación Autoruns es posible identificar que los únicos programas que se ejecutan automáticamente al iniciar el sistema corresponden a aplicaciones legítimas del sistema operativo. (Véase la figura 6.15)

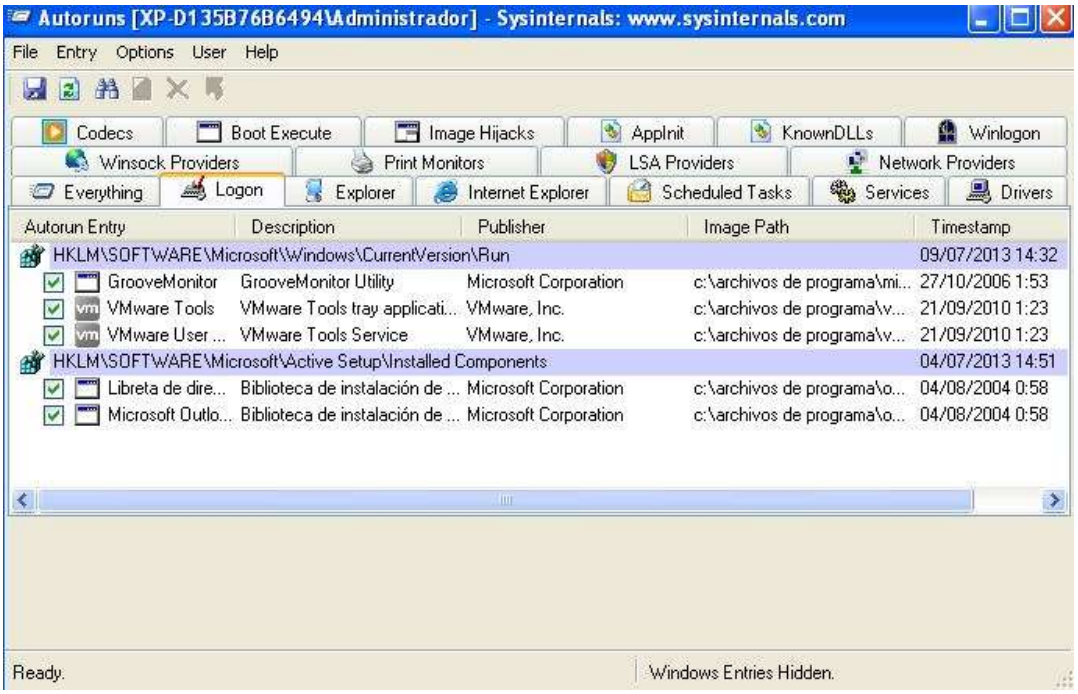


Figura 6.15 Aplicaciones legítimas ejecutadas al arranque del sistema operativo.

6.4.3. Paso 3. Infección del sistema virtual.

En este paso se ejecuta la aplicación maliciosa “descuentoCam.exe” en la máquina virtual recién instalada. Al realizar esta acción se observa que la aplicación maliciosa despliega una imagen que hace referencia a cámaras de video (véase la figura 6.16).

Figura 6.16 Imagen mostrada después de ejecutar la aplicación maliciosa.

6.4.4. Paso 4. Documentación del estado del sistema infectado.

Una vez que se ha infectado el equipo se realizan las mismas acciones señaladas en el paso 2, listar los procesos y conexiones red activos.

La figura 6.17 muestra los procesos en ejecución en el sistema infectado, puede observarse que hay un total de 27 procesos, entre esos procesos se encuentra "services.exe" con el PID 184.

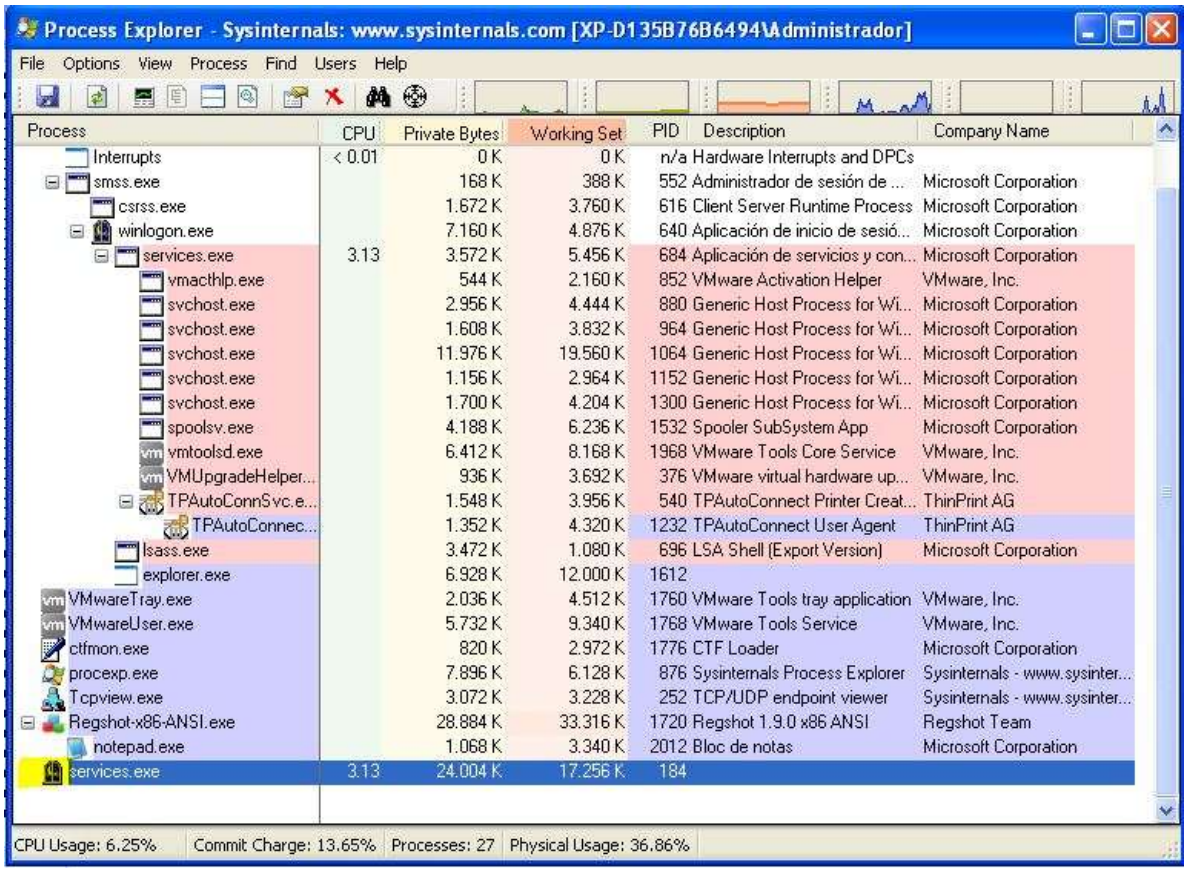


Figura 6.17 Procesos en ejecución en el sistema infectado.

Al revisar las conexiones de red para el sistema infectado se observa (Véase la figura 5.18) que no hay conexiones establecidas, sin embargo hay tres puertos a la escucha de conexiones entrantes, los puertos 5112, 51100 y 5110 han sido habilitados por el proceso con PID 184, "services.exe".

Al revisar los formatos generados en la fase de análisis en vivo de esta investigación (Véase Tabla 6.9 Información de las conexiones de red de proceso sospechoso.) se observa que el proceso “services.exe” ha establecido conexiones con un host remoto utilizando los mismos puertos no convencionales.

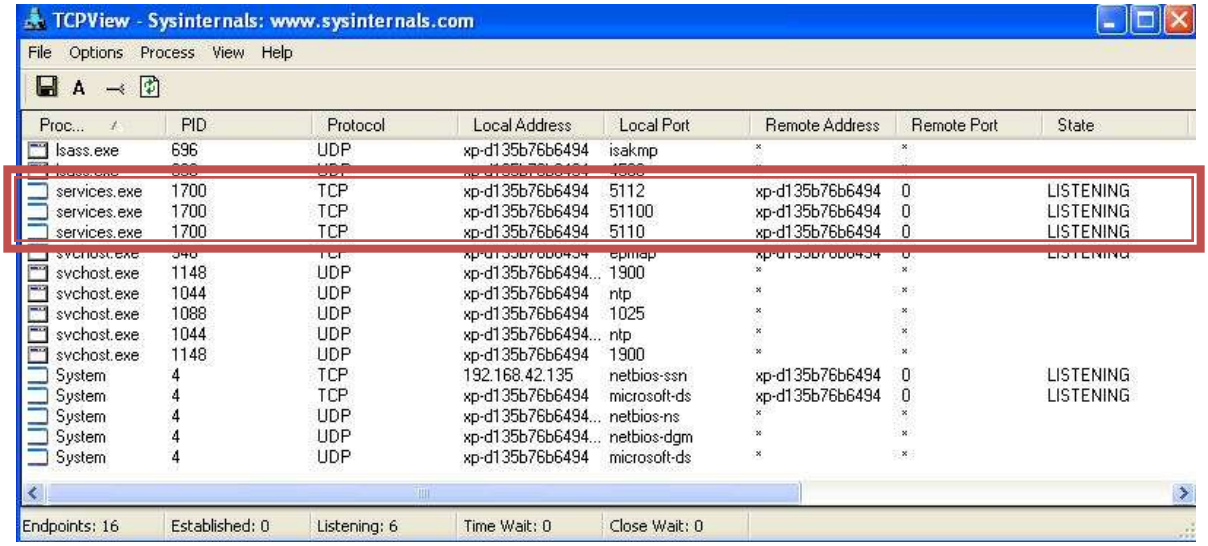


Figura 6.18 Conexiones de red del sistema infectado.

Si se listan las aplicaciones que se ejecutan al iniciar el sistema recién infectado (véase la figura 6.19) es posible identificar que la aplicación “fservice.exe” ubicada en la ruta “C:\windows\system32\” ha sido añadida a la lista, lo cual indica que éste programa es utilizado por el malware y es el responsable de levantar el proceso “services.exe”.

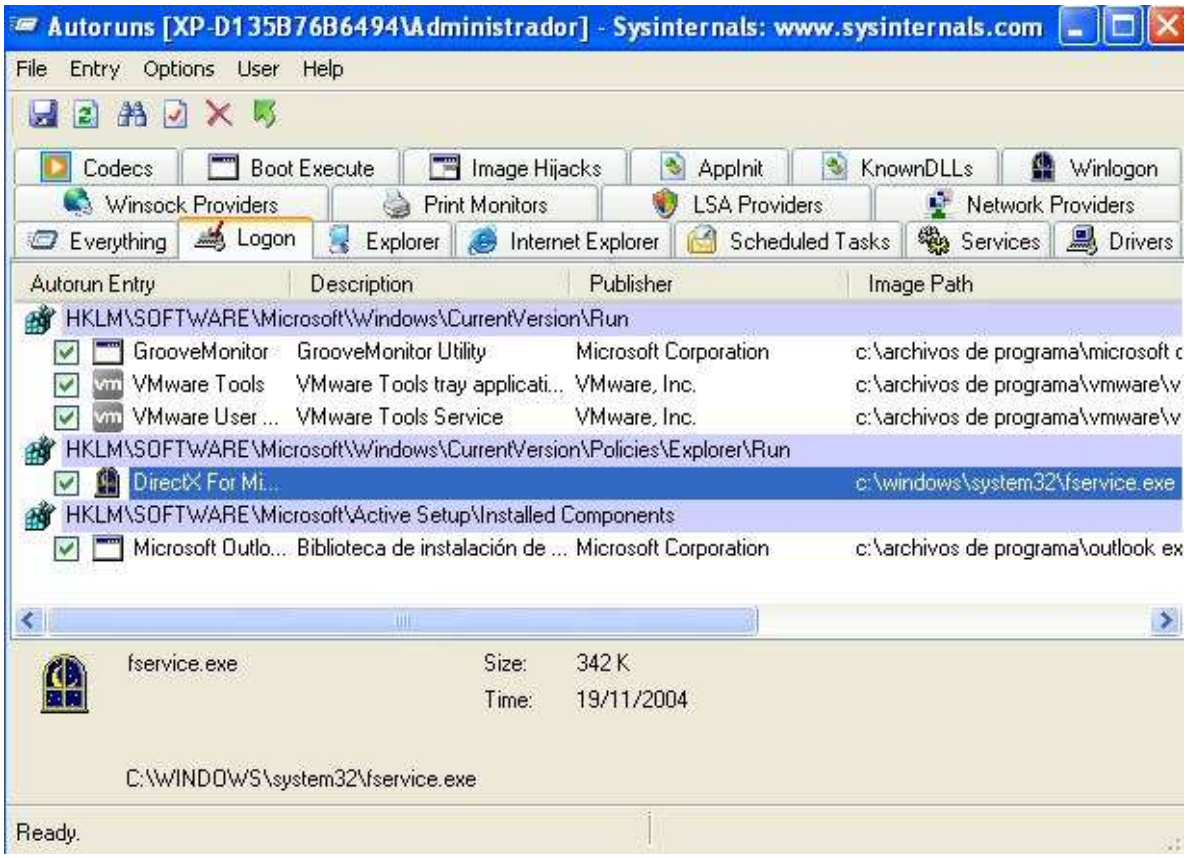


Figura 6.19 Aplicaciones ejecutadas al inicio del sistema infectado.

La identificación de este archivo ejecutable puede resultar de utilidad si es encontrado en el sistema investigado, al encontrarlo se obtiene mayor evidencia que ayude a respaldar una hipótesis. Por tal motivo es necesario registrar su firma MD5 para contar con una referencia de la identidad del archivo (véase la figura 6.20) y asentar toda la información relevante en la tabla 6.16.

```
D:\Lab\malware>fciv fservice.exe
//
// File Checksum Integrity Verifier version 2.05.
//
b732f616b18b992d350fd78e2ab97fb3 fservice.exe
```

Figura 6.20 Hash MD5 para el archivo “fservice.exe”.

Tabla 6.16 Información sobre el hallazgo “fservice.exe”.

Identificador del hallazgo	ANA-HED-05
Identificador del dispositivo origen	N/A (archivo encontrado en una prueba de concepto, análisis de malware)
Identificador del contenedor de hallazgos	LAB-DDE-01
Identificador de la cadena de custodia	CC-01
Descripción	Programa que se ejecuta en cada inicio del sistema, identificado en el análisis de malware
Nombre del archivo	fservice.exe
Hash MD5	b732f616b18b992d350fd78e2ab97fb3
Ubicación	C:\windows\system32\

6.4.5. Paso 5. Conclusiones del análisis básico de malware.

Con la información recolectada tras realizar el análisis se determina que existe una relación entre las aplicaciones maliciosas encontradas durante el análisis en vivo del sistema afectado. La aplicación “descuentosCam.exe” se trata de un troyano identificado como “ProRAT”, al ser ejecutada realiza cambios en el sistema, entre ellos la modificación de una llave de registro para ejecutar automáticamente el archivo “fservice.exe” copiado al sistema por el troyano.

El ejecutable “fservice.exe” es la puerta trasera encargada de brindar acceso al intruso. Al ser ejecutado crea un proceso llamado “services.exe” encargado de establecer conexiones con un equipo remoto. Estas conexiones son utilizadas para la transferencia de todo tipo de archivos entre ambos equipos, la ejecución de comandos de manera remota, entre otras acciones permitidas por el malware.

La conclusión obtenida tras realizar el análisis básico de malware apoya la hipótesis de que la fuga de información sucedió a causa de una aplicación maliciosa, por tal motivo es necesario continuar la investigación siguiendo el curso que plantea la reformulación de la hipótesis, es decir, el siguiente paso en la investigación es determinar cómo llegó el archivo “descuentosCam.exe” al equipo.

Para lograr tal propósito es posible comenzar a buscar información directamente en el equipo que continúa encendido y con el sistema operativo en ejecución, sin embargo al realizar la búsqueda de datos relevantes para la investigación bajo esas condiciones es posible que ocurra algún tipo de alteración o pérdida de la misma causada accidentalmente al revisar el sistema. Por tal motivo se recomienda implementar la metodología propuesta en este trabajo para el análisis de un sistema detenido.

6.5. Etapa de identificación, sistema detenido uno.

De acuerdo con la metodología establecida en este trabajo de investigación, los primeros pasos para realizar la investigación de un sistema detenido son conseguir autorización por escrito para iniciar el proceso de investigación, hacer entrega de una carta de confidencialidad y generar un formato con información general de la investigación. Estos puntos ya han sido cubiertos al iniciar la investigación del sistema en ejecución y aplican para esta sección, por lo que no es necesario desarrollarlos nuevamente.

Siendo así, el siguiente paso marcado en la metodología es la aplicación de un cuestionario que permite focalizar la búsqueda en función del activo afectado, ubicándolo y permitiendo establecer un plan de acción para continuar con la investigación. Sin embargo, para esta investigación en particular el activo afectado se tiene bien identificado, mientras que lo que se busca es información sobre un archivo malicioso.

Tomando esto en cuenta, es posible modificar el cuestionario para que las respuestas ofrezcan información relevante sobre el archivo malicioso. De la misma manera, las preguntas pueden modificarse para obtener información adicional sobre cualquier activo informático, incluso es posible añadir o eliminar preguntas según lo amerite la situación.

Las preguntas modificadas son las siguientes:

a) ¿Reconoce el archivo que tiene por nombre “descuentosCam”?
b) ¿Recuerda haber visto la imagen relacionada al archivo en cuestión?
c) ¿Quién interactuó con el archivo por primera vez?
d) ¿Algún conocido le compartió el archivo?
e) ¿Recuerda cómo llegó el archivo al equipo?

De acuerdo con las respuestas de Julieta Guerrero, responsable de la empresa, el archivo llegó como propaganda a la cuenta de correo contacto.sviw@gmail.com, tanto Julieta como Salvador Pedrosa cuentan con las credenciales de acceso a dicha cuenta, y ambos visualizaron el mensaje conjuntamente en el equipo analizado. Al ver que la imagen enviada no contenía información relevante para la empresa eliminaron el correo recibido. No hay mención de la fecha en la que esto sucedió.

Es recomendable añadir las preguntas que se considere necesarias para obtener información que ayude a la investigación, por ejemplo, ¿Qué navegador web utilizan comúnmente?

Al tratarse de un archivo adjunto enviado a una cuenta de correo de un servicio público, lo más probable es que hubiese sido descargado través de un navegador web, por lo que se debe de buscar el archivo que contiene el historial de navegación utilizado por el navegador correspondiente.

La metodología señala en este punto la documentación de la información recopilada relacionada al activo afectado, sin embargo puede adaptarse para documentar la información relacionada al activo de interés, el hallazgo de este activo puede servir para respaldar la hipótesis planteada. La tabla 6.17 muestra información relativa al activo de interés.

Tabla 6.17 Información del activo de interés.

Formato: IDEN-AIT-01	
Identificador del activo	AIT-001
Tipo de activo	Registro de historial de navegación de Mozilla Firefox. (places.sqlite)
Extensión	.sqlite
Software asociado	Mozila Firefox, SQLite Manager
Descripción	Registro de sitios web visitados, descargas realizadas, entre otra actividad de navegación web realizada con el explorador Mozilla Firefox.
Usuarios con acceso al archivo	Julieta Guerrero, Salvador Pedrosa
Equipo en el que está ubicado	*PC-009*
Responsable del activo	No aplica.

6.6. Etapa de preservación, sistema detenido uno.

Ya identificado el activo de información de interés es necesario iniciar los procedimientos para ubicarlo en el disco duro sospechoso, por tal motivo se debe generar una imagen forense en la cual trabajar, esta generación debe ser registrada en la bitácora correspondiente al disco duro sospechoso. La tabla 6.18 ejemplifica el registro de este procedimiento en la bitácora correspondiente.

Tabla 6.18 Bitácora de acceso al dispositivo PC-01-DD01.

Bitácora : *LOG-CC-02* correspondiente al dispositivo: *PC-01-D01* perteneciente a la Cadena de custodia: *CC-01* de la Investigación: *Caso B-201306-VSIW*						
Nombre del solicitante	Firma	Motivo	Fecha y hora de inicio	Fecha y hora de término	Autoriza	Firma de autorización
Demian García	ddd	Generación de imagen forense	21/06/2013 17:00hrs	21/06/2013 18:00hrs	Julieta Guerrero	xxx

Para realizar la imagen forense se utilizó la herramienta FTK Imager 3.1.20 la figura 6.21 muestra la interfaz principal de la herramienta.

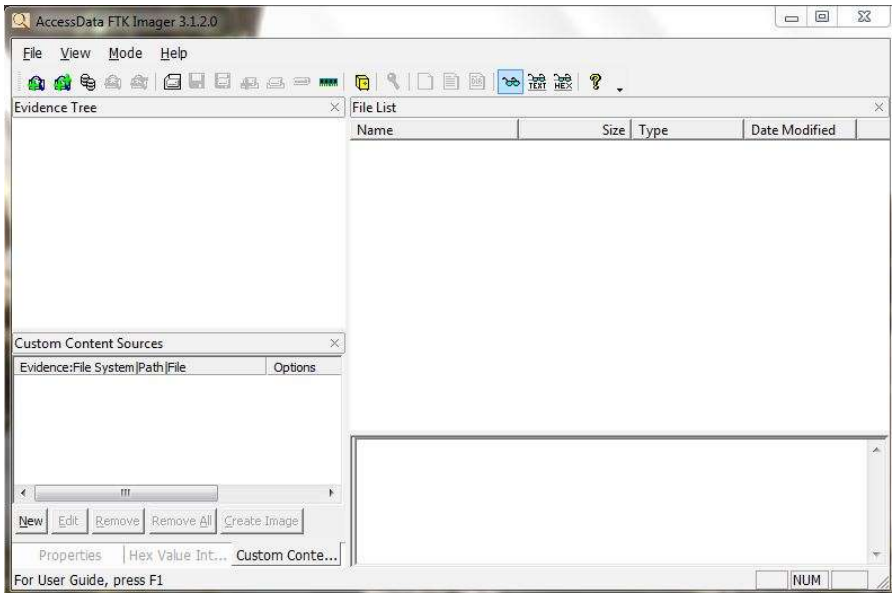


Figura 6.21 Interfaz principal de FTK Imager.

Para crear la imagen es necesario indicar la fuente que ha de ser copiada, en el menú “file” se selecciona la opción “Create Disk Image…” y se selecciona el tipo de dispositivo origen a copiar. En este caso es de tipo “Physical Drive” y está

conectado a través del puerto USB. La figura 6.22 muestra las ventanas correspondientes para los procedimientos antes mencionados.

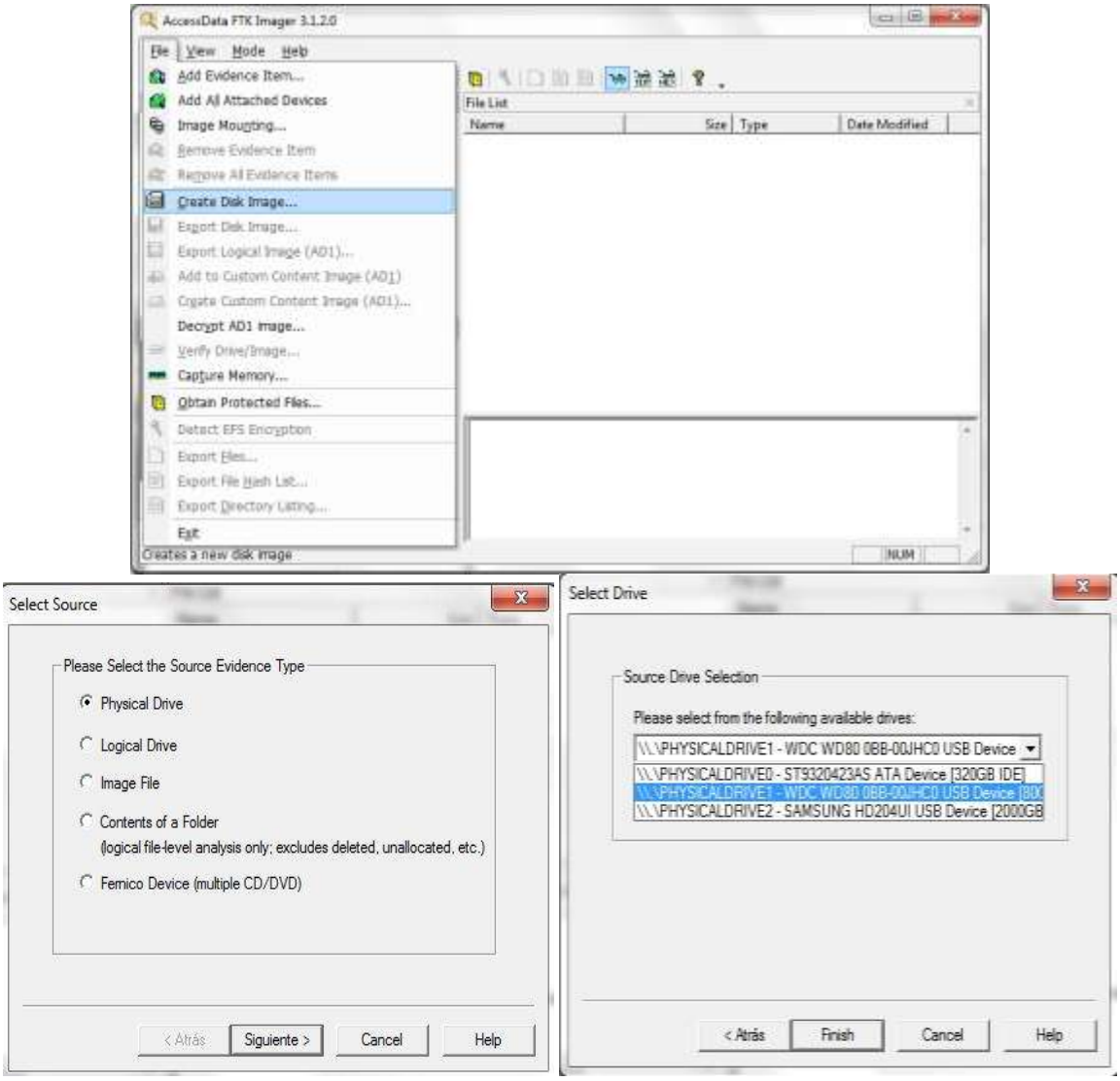


Figura 6.22 Selección de tipo de dispositivo origen.

Una vez que se selecciona el dispositivo orignal se debe elegir el tipo de archivo para la imagen forense, en este caso se eligió la extención “.E01”.

La hermienta FTK permite fragmentar la imagen forense en diferentes archivos de un tamaño establecido por el usuario, en este caso no se utilizó la fragmentación y se generó un sólo archivo. La figura 6.23 muestra la ventana con las opciones para guardar la imagen forense.

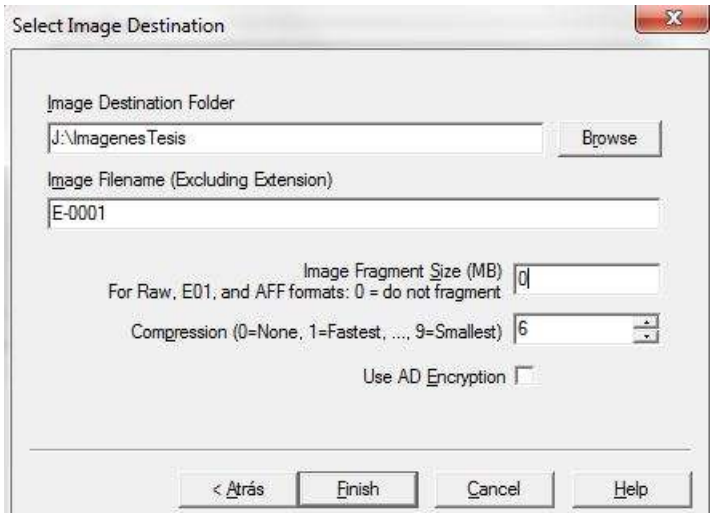


Figura 6.23 Selección del destino de la imagen y tamaño de los fragmentos.

Toda la información relacionada con el proceso de generación de imagen forense debe ser asentada en el formato correspondiente para contar con un respaldo por escrito de las acciones realizadas. La tabla 6.19 muestra el formato correspondiente con la información generada.

Tabla 6.19 Información referente a la generación de la imagen forense.

Formato: PRE-GIF-01	
Identificadores	
Identificador de la imagen forense	IMGF-PC-01-DD01
Identificador del dispositivo origen	PC-01-DD01
Identificador de la cadena de custodia a la que pertenece el dispositivo	CC-001
Identificador del dispositivo usado para almacenar la imagen	LAB-DDE-01
Información de la generación de la imagen	
Herramienta usada	FTK Imager
MD5 de la herramienta	f6d2c8f47461e589410a17c097c29385
MD5 de la imagen generada	ef6a7ab2afb99dfdb3218f9d35998130
Formato de la imagen	.E01

Tamaño de la imagen	81GB
Responsable de la generación del a imagen	Demian García
Firma del responsable	
Hora y fecha de la generación	21 agosto 2013, 18:00hrs
Identificado de la bitácora de hashes	HASH-PC-009-DD001

6.7. Etapa de análisis, sistema detenido uno.

Una vez que se ha generado la imagen forense es posible analizarla con la herramienta FTK Imager, entre las ventajas que presenta esta herramienta están el despliegue del contenido desglosado por las particiones en el disco y los datos del espacio no asignado, además de no modificar la evidencia y ofrecer una forma cómoda de visualizar la información contenida en la imagen forense.

Para visualizar el contenido de la imagen es necesario utilizar la opción “añadir evidencia” y seleccionar la opción “archivo de imagen” como se muestra en la figura 6.24.

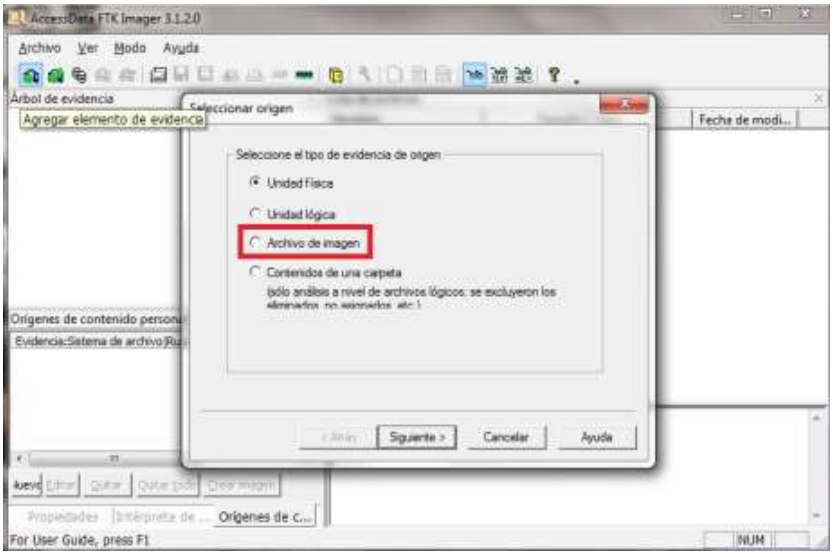


Figura 6.24 Interfaz para agregar elemento de evidencia.

Cuando la imagen forense es montada correctamente en la herramienta, la ventana principal muestra las particiones existentes en el disco duro sospechoso, incluyendo el espacio no particionado, en el lado izquierdo de la ventana mostrando la información como un árbol de directorios. La figura 6.25 muestra la vista de la imagen forense montada en la herramienta.

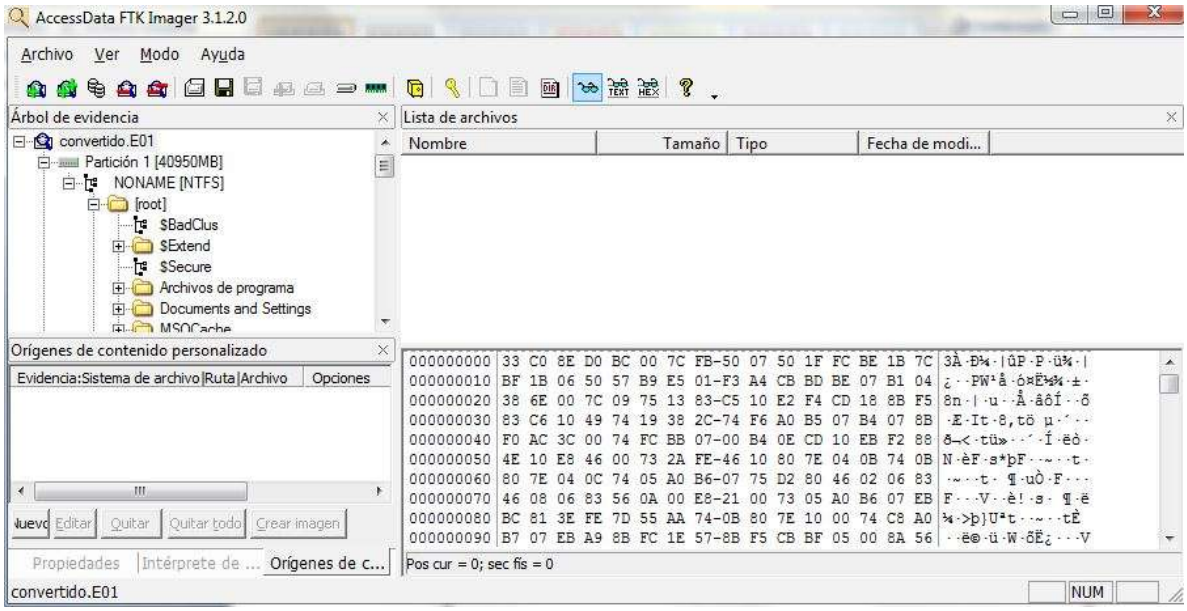


Figura 6.25 Elemento de evidencia correctamente montado.

De acuerdo a los resultados del análisis de malware es necesario identificar el archivo “fservice.exe” en el disco duro para comprobar que el equipo se encuentra infectado, por tal motivo basta con listar el contenido del directorio “C:\windows\system32\” a través de la herramienta FTK Imager para identificar el archivo malicioso (véase la figura 6.26).

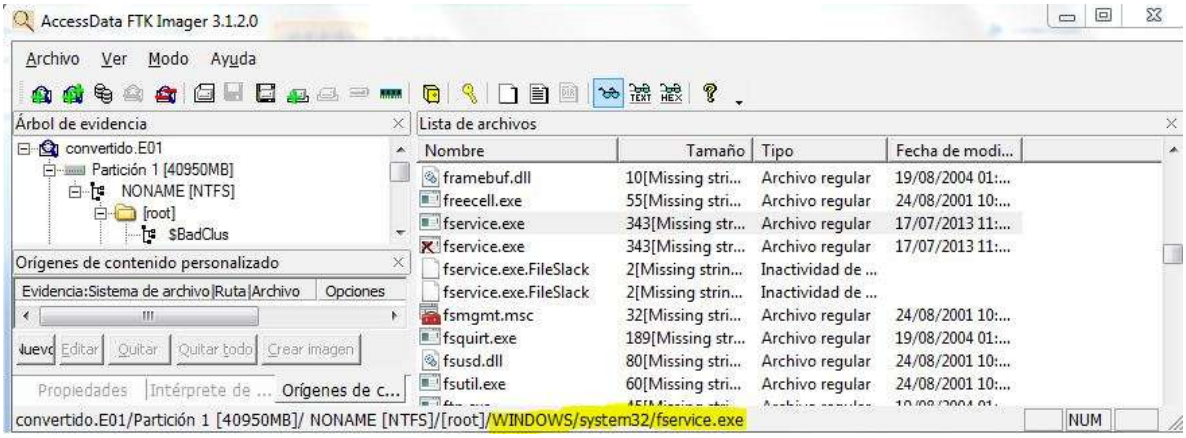


Figura 6.26 Archivo fservice.exe en el disco duro del sistema uno.

Una vez identificado el archivo es posible extraerlo de la imagen y obtener su firma hash MD5. Estos datos son documentados como parte del hallazgo en la tabla 6.20.

Tabla 6.20 Información sobre el hallazgo fservices.exe en el disco duro del sistema uno.

Identificador del hallazgo	ANA-HED-06
Identificador del dispositivo origen	PC-01-D01
Identificador del artefacto forense origen	IMGF-PC-01-DD01
Identificador del contenedor de hallazgos	LAB-DDE-01
Descripción	Archivo maliciosa que se ejecuta en cada inicio del sistema, encontrado en el disco duro del sistema uno.
Nombre del archivo	fservices.exe
Ubicación del archivo	C:\windows\system32\
Hash MD5	b732f616b18b992d350fd78e2ab97fb3

Una vez que se ha documentado este hallazgo es posible continuar la revisión de los datos contenidos en la imagen forense en busca del archivo “places.sqlite” que

contiene el historial de navegación del explorador Mozilla Firefox. La búsqueda de éste archivo en particular fue determinada por las modificaciones al cuestionario presentado en la metodología.

De acuerdo con documentación oficial de Mozilla[32] el archivo "places.sqlite" se ubica en "*C:\Documents and Settings\<Windows login/user name>\Application Data\Mozilla\Firefox\Profiles\<profile folder>"*

La figura 6.27 muestra que el archivo en cuestión se encuentra en la ubicación indicada dentro de la imagen forense generada.

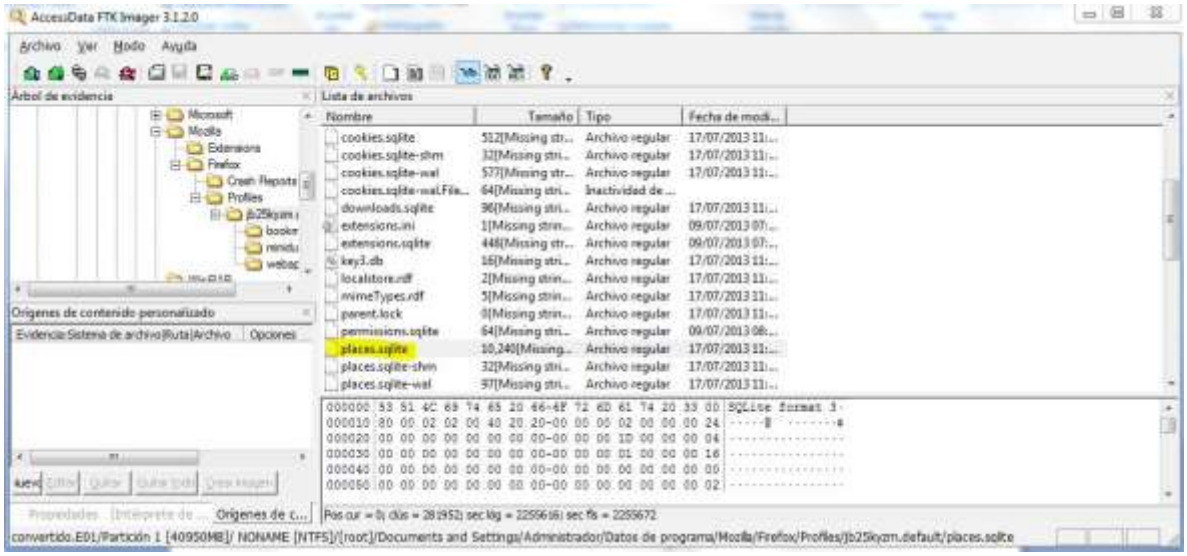


Figura 6.27 Ubicación del archivo "places.sqlite" en la imagen forense.

Una vez ubicado el archivo se procede a extraerlo de la imagen para analizarlo. La herramienta FTK Imager permite exportar el archivo a una carpeta local, sólo hace falta un clic derecho sobre el archivo de interés y seleccionar la opción "Exportar archivos…" (véase la figura 6.28)

[32] http://kb.mozillazine.org/Profile_folder_-_Firefox

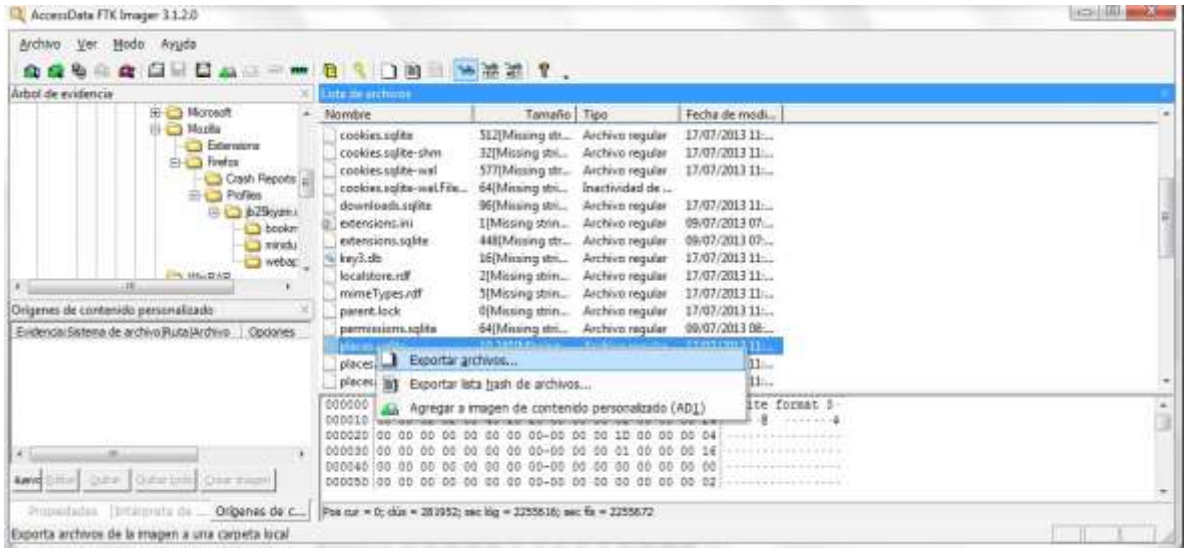


Figura 6.28 Exportar “places.sqlite” a una carpeta local.

Se recomienda que también se exporte la lista de hash del archivo para documentar el valor del hash y demostrar que el archivo exportado es el mismo que está alojado en la imagen forense.

Después de realizar la comprobación de firmas hash es posible añadir al archivo “places.sqlite” como un hallazgo relevante para el caso, por tal motivo se documenta la información relacionada al archivo como se muestra en la tabla 6.21

Tabla 6.21 Información sobre el hallazgo “places.sqlite”.

Identificador del hallazgo	ANA-HED-07
Identificador del dispositivo origen	PC-01-D01
Identificador del artefacto forense origen	IMGF-PC-01-DD01
Identificador del contenedor de hallazgos	LAB-DDE-01
Descripción	Archivo que contiene el historial de navegación de Mozilla Firefox correspondiente a la cuenta de usuario

	"Administrador"
Nombre del archivo	places.sqlite
Ubicación del archivo	C:\Documents and Settings\Administrador\ Datos de programa\Mozilla\Firefox\Profiles\ jb25kyzm.default\
Hash MD5	5a57aefb4ab3e8d442b895032ac07b0c

Una vez que se ha exportado el archivo es posible consultarlo con la herramienta especializada "MozillaHistoryView"[33], esta herramienta ofrece una visualización de los contenidos registrados en el historial del navegador. Para utilizarla basta con descargar la aplicación del sitio oficial y seleccionar el archivo "places.sqlite". (véase la figura 6.29)

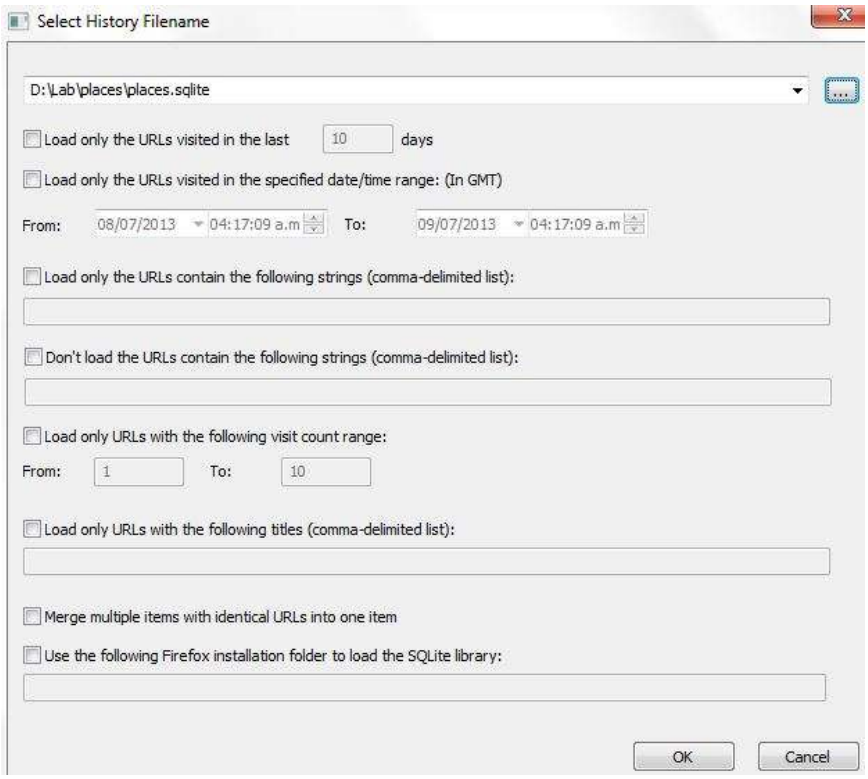


Figura 6.29 Selección de archivo .sqlite para la aplicación MozillaHistoryView.

[33] http://www.nirsoft.net/utils/mozilla_history_view.html

La interfaz de la herramienta muestra el contenido del historial ordenado en diferentes columnas, entre ellas URL, primera y última visita, un contador de visitas, título de la página, tipo de visita, entre otros. (Véase la figura 6.30)

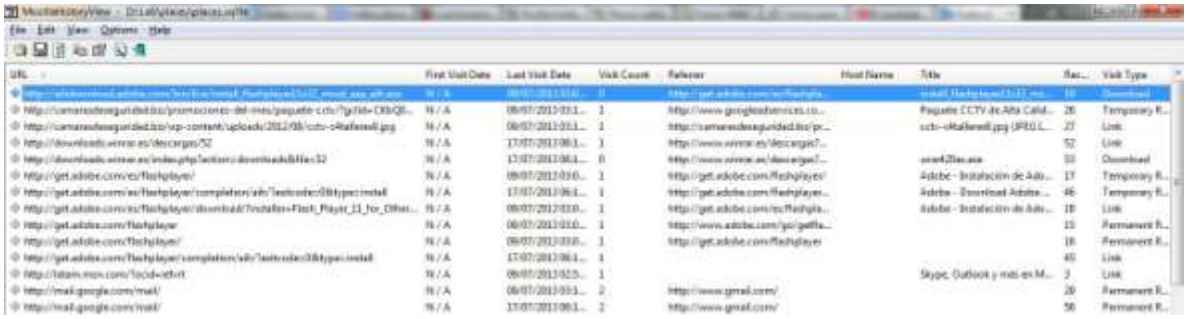
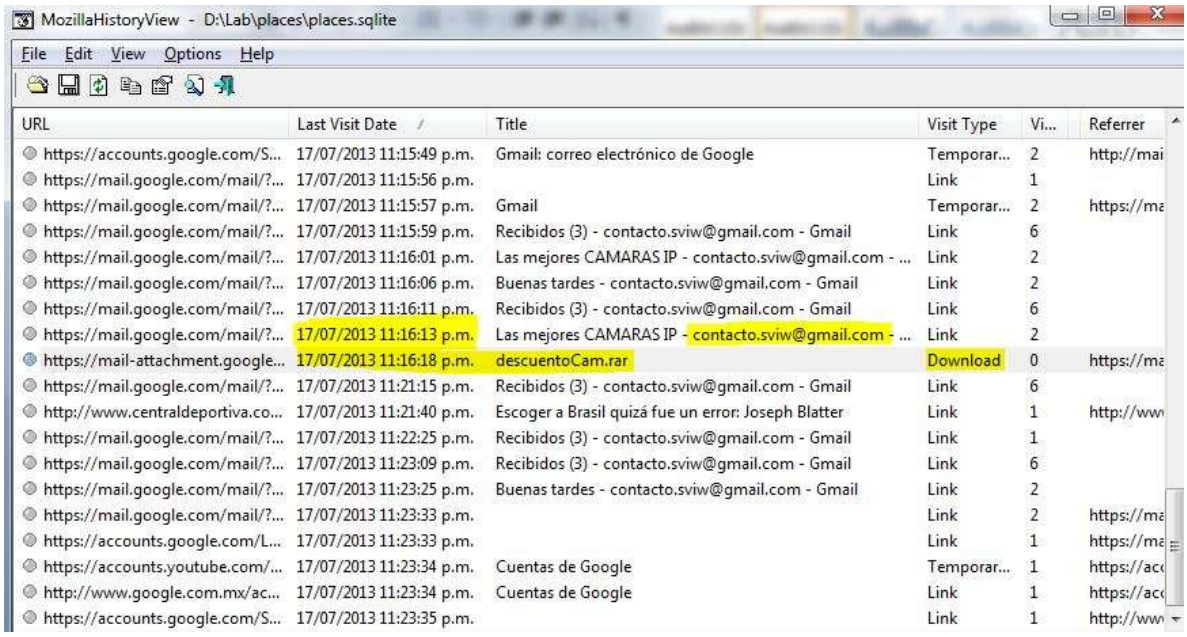


Figura 6.30 Interfaz de la herramienta MozillaHistoryView.

Al analizar el contenido del historial es posible identificar actividad relacionada con la cuenta de correo “contacto.sviw@gmail.com”, la actividad identificada se trata de la descarga de un archivo adjunto, “descuentoCam.rar”, el día 17 de julio de 2013 a las 11:16:18 pm. (Véase la figura 6.31).



URL	Last Visit Date	Title	Visit Type	Vi...	Referrer
https://accounts.google.com/S...	17/07/2013 11:15:49 p.m.	Gmail: correo electrónico de Google	Temporar...	2	http://mai
https://mail.google.com/mail/?...	17/07/2013 11:15:56 p.m.		Link	1	
https://mail.google.com/mail/?...	17/07/2013 11:15:57 p.m.	Gmail	Temporar...	2	https://ma
https://mail.google.com/mail/?...	17/07/2013 11:15:59 p.m.	Recibidos (3) - contacto.sviw@gmail.com - Gmail	Link	6	
https://mail.google.com/mail/?...	17/07/2013 11:16:01 p.m.	Las mejores CAMARAS IP - contacto.sviw@gmail.com - ...	Link	2	
https://mail.google.com/mail/?...	17/07/2013 11:16:06 p.m.	Buenas tardes - contacto.sviw@gmail.com - Gmail	Link	2	
https://mail.google.com/mail/?...	17/07/2013 11:16:11 p.m.	Recibidos (3) - contacto.sviw@gmail.com - Gmail	Link	6	
https://mail.google.com/mail/?...	17/07/2013 11:16:13 p.m.	Las mejores CAMARAS IP - contacto.sviw@gmail.com - ...	Link	2	
https://mail-attachment.google...	17/07/2013 11:16:18 p.m.	descuentoCam.rar	Download	0	https://ma
https://mail.google.com/mail/?...	17/07/2013 11:21:15 p.m.	Recibidos (3) - contacto.sviw@gmail.com - Gmail	Link	6	
http://www.centraldeportiva.co...	17/07/2013 11:21:40 p.m.	Escoger a Brasil quizá fue un error: Joseph Blatter	Link	1	http://ww
https://mail.google.com/mail/?...	17/07/2013 11:22:25 p.m.	Recibidos (3) - contacto.sviw@gmail.com - Gmail	Link	1	
https://mail.google.com/mail/?...	17/07/2013 11:23:09 p.m.	Recibidos (3) - contacto.sviw@gmail.com - Gmail	Link	6	
https://mail.google.com/mail/?...	17/07/2013 11:23:25 p.m.	Buenas tardes - contacto.sviw@gmail.com - Gmail	Link	2	
https://mail.google.com/mail/?...	17/07/2013 11:23:33 p.m.		Link	2	https://ma
https://accounts.google.com/L...	17/07/2013 11:23:33 p.m.		Link	1	https://ma
https://accounts.youtube.com/...	17/07/2013 11:23:34 p.m.	Cuentas de Google	Temporar...	1	https://ac
http://www.google.com.mx/ac...	17/07/2013 11:23:34 p.m.	Cuentas de Google	Link	1	https://ac
https://accounts.google.com/S...	17/07/2013 11:23:35 p.m.		Link	1	http://ww

Figura 6.31 Descarga del archivo “descuentoCam.rar”.

Este hallazgo confirma que el archivo malicioso llegó al equipo a través de un correo electrónico. Al revisar el contenido de la carpeta de descargas en la imagen forense se puede apreciar que la aplicación maliciosa fue descomprimida el mismo día a las 11:18:18pm, es decir, un par de minutos después de descargar el archivo adjunto, (véase la figura 6.32), por tal motivo este hallazgo se documenta como se muestra en la tabla 6.22.

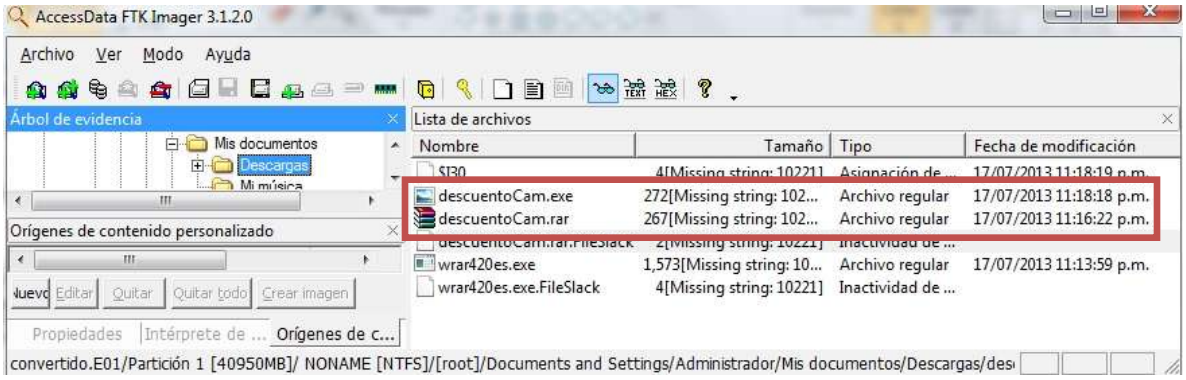


Figura 6.32 Última modificación de la aplicación maliciosa.

Tabla 6.22 Información sobre el hallazgo “descuentosCam.exe”.

Identificador del hallazgo	ANA-HED-08
Identificador del dispositivo origen	PC-01-D01
Identificador del artefacto forense origen	IMGF-PC-01-DD01
Identificador del contenedor de hallazgos	LAB-DDE-01
Descripción	Aplicación maliciosa identificada en el disco duro del sistema uno, misma aplicación que fue analizada previamente.
Nombre del archivo	descuentosCam.exe
Ubicación del archivo	C:\Documents and Settings\Administrador\ Mis documentos\Descargas\
Hash MD5	1072f5cee0640caaefa48843eda6614c

Hasta este punto de la investigación se ha demostrado que una aplicación maliciosa levanta un proceso que permite conexiones remotas, la aplicación se ha identificado como un troyano que facilita a un intruso tener acceso al equipo para consultar archivos, descargar, modificar, crear o eliminar contenido en el sistema, así como ejecutar comandos de manera remota. No hay evidencia que demuestre que la aplicación maliciosa haya sido utilizada para robar los archivos confidenciales, sin embargo, las fechas de modificación de los archivos que contienen las licitaciones son más recientes que la llegada del malware (véase la figura 6.33) por lo que no se puede descartar el uso del troyano para robar la información.

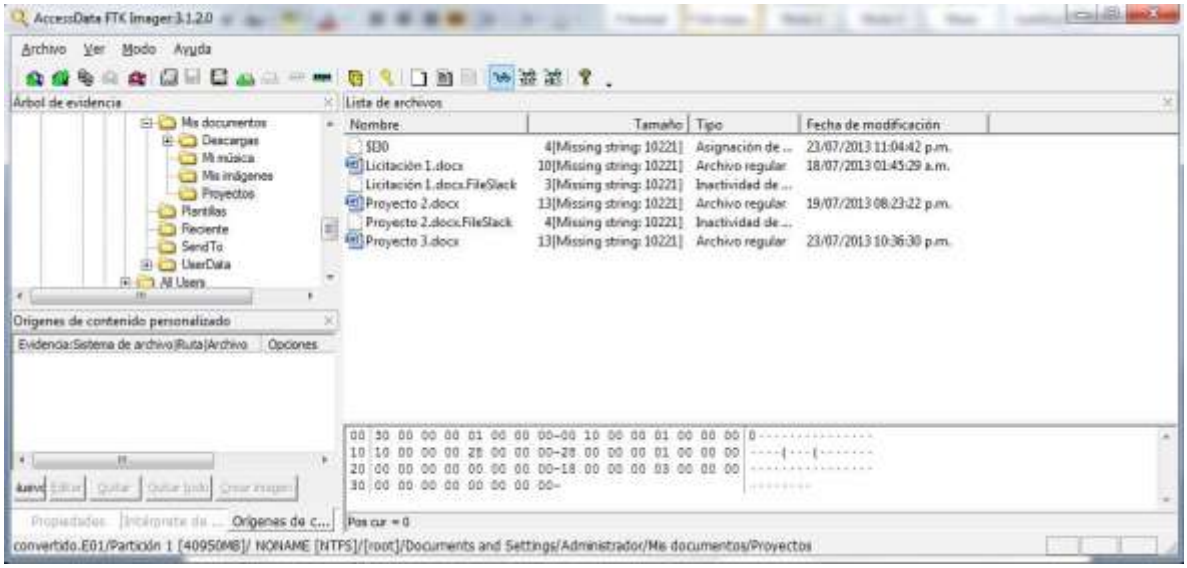


Figura 6.33 Fechas de modificación de archivos confidenciales.

Es necesario determinar el origen del correo electrónico para continuar con la investigación, sin embargo el correo que contenía la aplicación comprimida fue eliminado y no es posible recuperarlo. Debido a que el servicio de correo es proporcionado por una empresa ajena a la empresa Seguridad y Vigilancia iW es poco probable que el correo eliminado pueda ser recuperado una vez removido de la cuenta correspondiente.

En caso de que la evidencia no hubiese sido alterada, la investigación continuaría al revisar el contenido de la cabecera del correo malicioso, en especial el campo “Recived”, el cual indica el camino que siguió el correo desde su origen. Este tipo de investigación requeriría colaboración con proveedores de servicio de internet o alguna otra entidad para ubicar al usuario que utilizó la IP origen el día y la fecha establecida en el correo.

La persona responsable de eliminar el correo fue la Ing. Julieta Guerreo después de leer el mensaje en su estación de trabajo. Esta persona tiene acceso a los documentos filtrados y existen copias almacenadas en su equipo, por lo que es importante investigar el sistema para determinar si la fuga de información se produjo desde su estación de trabajo. Al momento de la investigación su equipo se encuentra apagado, por lo que se realiza una investigación para un sistema detenido.

6.8. Etapa de identificación, sistema detenido dos.

El objetivo de la investigación es identificar la forma en que se filtró la información confidencial. Hasta el momento se sabe que el equipo de cómputo utilizado por el Ing. Salvador Pedrosa se encuentra infectado con malware que permite acceso al sistema de forma remota, la infección fue producida por un programa malicioso enviado por correo, mismo correo que presuntamente fue desplegado en el sistema de la Ing. Julieta Guerrero.

Toda la información recolectada en el transcurso de la investigación sirve como base para plantear una primera hipótesis: El equipo de la Ing. Guerrero se encuentra infectado con el mismo malware que facilita el robo de información a través de conexiones no autorizadas.

Para probar esta hipótesis es necesario demostrar que el archivo “descuentosCam.exe” con identificador de hallazgo ANA-HED-08 fue ejecutado en

el equipo con identificador PC-02 perteneciente a la Ing. Julieta Guerrero. Sí se demuestra que fue ejecutado entonces se debe determinar cómo llegó al sistema.

Antes de iniciar con las actividades técnicas de la investigación se deben de seguir los pasos establecidos en la metodología para llevar un control documental de las acciones realizadas para obtener la evidencia digital.

Los primeros pasos mencionados en la metodología son:

- Conseguir autorización por escrito para iniciar el proceso de investigación.
- Hacer entrega de una carta de confidencialidad.
- Generar un formato con información general de la investigación.

Debido a que el equipo con identificador PC-02 utilizado por la Ing. Julieta Guerrero no fue contemplado en el alcance inicial de la investigación, es necesario conseguir la autorización expresa para trabajar con ese equipo. A diferencia de la carta de autorización, la carta de confidencialidad y el formato con información general de la investigación son documentos válidos para este proceso y no es necesario generar unos nuevos.

A continuación la carta de autorización para la estación de trabajo PC-02:

Carta de Autorización de Inicio de la Investigación
Fecha: 21 de agosto de 2013 Por medio de la presente se concede autorización expresa por parte del representante de la empresa **Seguridad y Viglancia iW**, **Ing. Julieta Guerrero**, al equipo de investigación liderado por, **Demian García**, para iniciar la investigación en cómputo forense con identificador: **Caso B-201306-SVIW**.

La investigación contempla la revisión de la estación de trabajo **Dell-DSK1200** con número de serie: **5478941177**. Con disco duro marca: **SeaGate** modelo: **SG-3951c** con capacidad de: **80GB** y número de serie: **3259234132-ERC-124**.

Así mismo, el representante de la empresa se compromete a apoyar y proveer todas las facilidades necesarias al equipo de investigación para que éste pueda llevar cabo la tarea sin complicaciones.

_____ _____

Firma del representante de la empresa Firma del líder de la investigación.

El siguiente paso marcado en la metodología es la aplicación de un cuestionario que permita focalizar la búsqueda en función del activo de interés, en este caso en particular dichos activos se tienen bien identificados, uno es el malware posiblemente instalado en el sistema, el otro activo de interés es el historial de navegación necesario para demostrar que el archivo malicioso fue descargado desde la cuenta de correo

Inicialmente el cuestionario está dirigido al usuario del equipo involucrado en el incidente, en este caso, después de la información recopilada durante la investigación es posible complementar el cuestionario con los datos obtenidos hasta el momento.

Las preguntas correspondientes a este cuestionario son:

a) ¿Qué tipo de archivos se requiere buscar?
b) ¿Cuáles son los nombres de los archivos a buscar?
c) ¿En qué ubicación se encuentran alojados?
d) ¿A qué usuario pertenecen?
e) ¿Qué navegador web utiliza el usuario?

La información recopilada se condensa en el Formato IDE-AIT-02 (véase la tabla 6.23).

Tabla 6.23 Información de los activos de interés.

Formato: IDE-AIT-02	
Identificador del activo	AIT-02
Tipo de activo	Malware que permite conexiones no autorizadas y lleva por nombre "fservice.exe"
Extensión	.exe
Software asociado	Sistema operativo
Descripción	Malware instalado por el troyano enviado por correo "descuentosCam.exe". Ubicado en: C:\windows\system32\
Usuarios con acceso al archivo	Julieta Guerrero
Equipo en el que está ubicado	*PC-02*
Responsable del activo	No aplica.
Identificador del activo	AIT-03
Tipo de activo	Registro de historial de navegación de Google Chrome. (places.sqlite)
Extensión	.sqlite
Software asociado	Google Chrome, SQLite Manager
Descripción	Registro de sitios web visitados,

	descargas realizadas, entre otra actividad de navegación web realizada con el explorador Google Chome. Ubicado en: C:\Documents and Settings\Adminsitrador\Local Settings\Application Data\Google\Chrome\User Data\Default\
Usuarios con acceso al archivo	Julieta Guerrero
Equipo en el que está ubicado	*PC-02*
Responsable del activo	No aplica.

El siguiente paso en el proceso de investigación es la implementación del proceso de cadena de custodia para la estación de trabajo de la Ing. Julieta Guerrero. La tabla 6.24 recopila la información del equipo en cuestión.

Tabla 6.24 Información relacionada al dispositivo involucrado en el incidente de seguridad.

Formato: IDE-HWD-01	
Tipo de dispositivo	Estación de Trabajo (PC)
Identificador del dispositivo	PC-02
Marca/Modelo	Dell-DSK1200
Número de Serie	5478941177
Características Generales	Computadora de escritorio marca Dell, gabinete color gris.
¿El equipo se encuentra encendido?	Equipo apagado.
Disco Duro asociado al equipo(1)	
Identificador del disco duro	PC-02-DD02

Marca	SeaGate
Modelo	SG-3951c
Número de serie	3259234132-ERC-124
Capacidad de almacenamiento	80 GB
Tipo de Interfaz	IDE
Ubicación del equipo	
Área a la que pertenece	Dirección General
Empresa/Organización	Seguridad y Vigilancia iw
Dirección	Calle 84 #131 Col. Nápoles. DF
Información adicional	N/A
Responsable del equipo	
Nombre del responsable	Ing. Julieta Guerrero
Nombre de usuario	
Puesto	
Correo electrónico	jguerrero@mail.com
Teléfono	551149301777
Descripción de actividades	Diseño y presentación de propuestas para realización de proyectos.
Conectividad	
Red a la que se conecta el equipo	Red SVIW
Tipo de conexión	Alámbrica, cable Ethernet

6.9. Etapa de preservación, sistema detenido dos.

El Formato: PRE-CC-01 muestra los datos de los dispositivos incluidos en la cadena de custodia en el transcurso de la investigación, se actualiza este formato al agregar los datos del dispositivo de almacenamiento del equipo con identificador PC-02 (véase la tabla 6.25).

Tabla 6.25 Información general relacionada con el proceso de la cadena de custodia.

Formato: PRE-CC-01	
Identificador de la cadena de custodia	CC-001
Identificador de la investigación	Caso B-201306-VSIW
Identificador del custodio asignado	ICF-DGV-201306
Descripción de los dispositivos	Dispositivo 1: Archivo de volcado del contenido de memoria RAM del sistema utilizado por Salvador Pedrosa. Dispositivo 2: Disco duro de 80 GB que contiene sistema operativo y datos del usuario Salvador Pedrosa. Dispositivo 3: Disco duro para almacenar evidencia e imágenes forenses. Dispositivo 4: Disco duro de 80 GB que contiene sistema operativo y datos del usuario Julieta Guerrero
Datos del dispositivo 1	
Identificador del dispositivo	MDUMP-PC-001-RAM001
Bitácora asociada	LOG-CC-01
Fecha y hora de inserción a la cadena	21/06/2013 16:00hrs
Datos del dispositivo 2	
Identificador del dispositivo	PC-01-D01
Bitácora asociada	LOG-CC-02
Fecha y hora de inserción a la cadena	21/06/2013 16:00hrs
Datos del dispositivo 3	
Identificador del dispositivo	LAB-DDE-01
Bitácora asignada	LOG-CC-03
Fecha y hora de inserción a la cadena	21/06/2013 16:00hrs

Datos del dispositivo 4	
Identificador del dispositivo	PC-02-DD01
Bitácora asociada	LOG-CC-04
Fecha y hora de inserción a la cadena	22/08/2013 12:49hrs

Una vez que el dispositivo ha sido contemplado en la cadena de custodia es necesario llevar un registro de todas las interacciones del equipo de investigación y el dispositivo. Por tal motivo se utiliza la bitácora LOG-CC-004 como se muestra en la tabla 6.26.

Tabla 6.26 Bitácora para el dispositivo PC-02-DD01.

Bitácora : LOG-CC-004 correspondiente al dispositivo: PC-02-D01 perteneciente a la Cadena de custodia: IDEN21-CC-001 de la Investigación: Caso B-201306-VSIW							
Nombre y procedencia del solicitante	Motivo	Traslado	Fecha y hora de inicio	Fecha y hora de término	Firma	Autorizado por	Firma
Demian García, Líder de la investigación	Obtención de imagen forense	Sin traslado	22/08/2013 12:49hrs	22/08/2013 14:00hrs		Julieta Guerrero	
Demian García, Líder de la investigación	Obtención de una segunda imagen forense	Sin traslado	22/08/2013 14:49hrs	22/08/2013 16:00hrs		Julieta Guerrero	

Continuando con el proceso de preservación, se genera la imagen forense del dispositivo PC-02-DD01 utilizando la aplicación FTK Imager. El proceso es el mismo que el realizado en el primer sistema. Toda la información relacionada con este proceso es asentada en el formato PRE-GIF-02 (véase la tabla 6.27).

Tabla 6.27 Información referente a la generación de la imagen forense.

Formato: PRE-GIF-02	
Identificadores	
Identificador de la imagen forense	IMGF-PC-02-DD01
Identificador del dispositivo origen	PC-02-DD02
Identificador de la cadena de custodia a la que pertenece el dispositivo	CC-002
Identificador del dispositivo donde se aloja la imagen	LAB-DDE-01
Información de la generación de la imagen	
Herramienta usada	FTK Imager
MD5 de la herramienta	f6d2c8f47461e589410a17c097c29385
MD5 de la imagen generada	b1d7861bb4090b3ee2b5b4501d1f22f8
Formato de la imagen	.E01
Tamaño de la imagen	81GB
Responsable de la generación del a imagen	Demian García
Firma del responsable	
Hora y fecha de la generación	22/08/2013, 12:49hrs
Identificado de la bitácora de hashes	HASH-PC-02-DD01

6.10. Etapa de análisis, sistema detenido dos.

Una vez que se ha generado la imagen forense comienza el proceso de análisis, este proceso incluye las actividades necesarias para validar la hipótesis planteada, en este caso la hipótesis implica identificar el archivo malicioso “descuentosCam.exe” documentado en el formato ANA-HED-04, prestando especial atención en el valor HASH MD5 para confirmar que se trata del mismo archivo malicioso.

De acuerdo al análisis de malware realizado anteriormente, al ejecutar el troyano se generan cambios en algunas llaves del registro de Windows con la intención de ejecutar la aplicación “C:\windows\system32\fservice.exe” al iniciar el sistema, de tal manera que de ser posible identificar estos elementos en la imagen forense se puede afirmar que el equipo está infectado.

Para identificar la aplicación maliciosa “fservice.exe”, basta con acceder al directorio correspondiente en la imagen forense y comprobar que la aplicación está ahí (véase la figura 6.34).

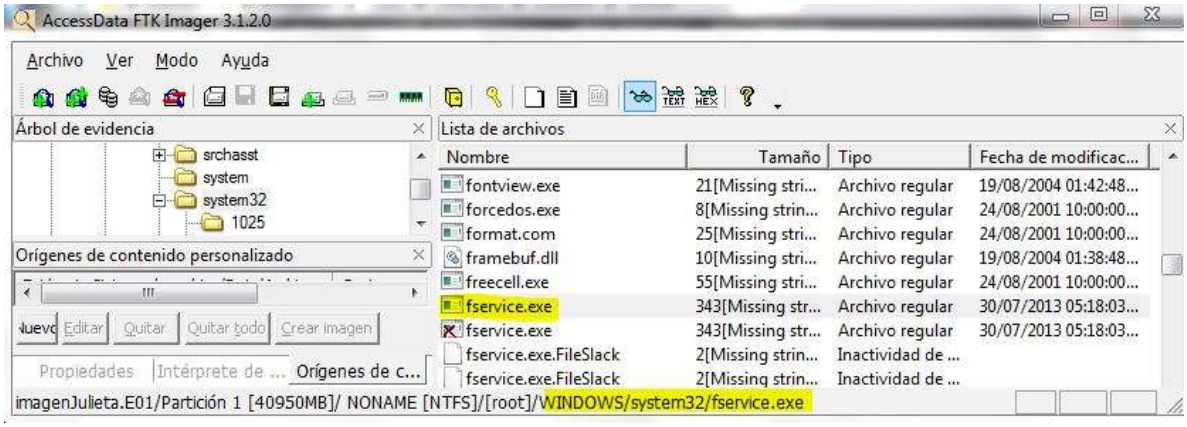


Figura 6.34 Ubicación del malware “fservice.exe”.

Un vez que se ha ubicado el archivo, se debe obtener su hash MD5 para asegurar que se trata del mismo archivo malicioso identificado en el sistema del Ing. Salvador Pedrosa, así como en el análisis de malware. Para ello es necesario extraer el archivo de la imagen forense, consultar el valor del hash MD5 (véase la

figura 6.35) y añadir el hallazgo a la documentación de evidencia encontrada (véase la tabla 6.28).

Figura 6.35 Hash MD5 del archivo “fserive.exe” encontrado en el equipo de Julieta Guerrero.

Tabla 6.28 Información sobre el hallazgo “fservices.exe”.

Identificador del hallazgo	ANA-HED-09
Identificador del dispositivo origen	PC-02-D01
Identificador del artefacto forense origen	IMGF-PC-02-DD01
Identificador del contenedor de hallazgos	LAB-DDE-01
Descripción	Programa malicioso que se ejecuta en cada inicio del sistema, permite conexiones remotas, identificado en el disco duro del sistema dos.
Nombre del archivo	fservices.exe
Ubicación del archivo	C:\windows\system32\
Hash MD5	b732f616b18b992d350fd78e2ab97fb3

Al comparar el valor del Hash MD5 del hallazgo ANA-HED-06, correspondiente al hash del archivo “fservice.exe” encontrado en el equipo de Salvador Pedrosa, con el hash mostrado en la figura 6.35 se puede apreciar que los valores son idénticos, lo que indica que se trata del mismo archivo. Por tanto se concluye que el troyano fue ejecutado e infectó el equipo de Julieta Guerrero. Es necesario ubicar el valor en la llave de registro correspondiente para demostrar que el malware se ejecuta en cada inicio del sistema, dejándolo listo para conexiones no autorizadas.

El registro de Windows es una base de datos estructurada que almacena valores de configuración del sistema. Estos valores son almacenados en diferentes archivos ubicados en “C:\windows\system32\config\software\” de donde son leídos e interpretados cuando el sistema arranca y se mantiene en ejecución. Al acceder a esa ubicación en la imagen forense, es posible identificar el archivo “software” (véase la figura 6.36), el cual contiene la llave de registro que se modifica para permitir la ejecución del malware. En el análisis de malware se identificó que al ejecutar el malware se añadía un valor en la llave de registro “HKLM\SOTWARE\Microsoft\Windows\CurrenteVersion\Policies\Explorer\Run”.

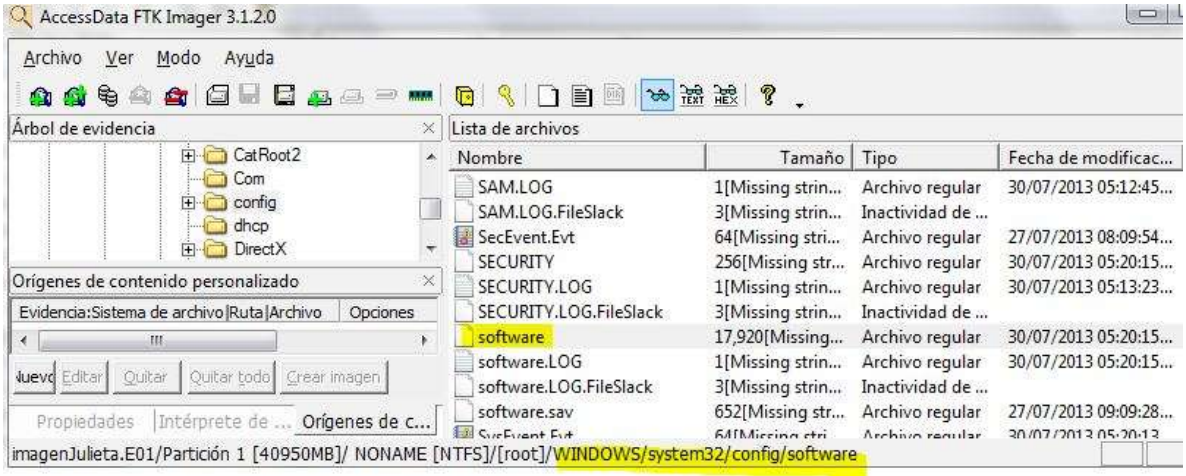


Figura 6.36 Ubicación del archivo “software” en la imagen forense.

Para consultar que el valor añadido por el troyano existe, es necesario extraer el archivo “software” de la imagen forense y utilizar alguna aplicación capaz de interpretar el contenido del archivo sin que modifique el mismo. Para comprobar que no hay modificación después de utilizar cualquier aplicación se obtiene el hash MD5 del archivo “software” (véase la figura 6.37) después de extraerlo de la imagen forense.

Figura 6.37 Hash MD5 del archivo “software” recién extraído de la imagen forense.

El archivo es documentado como parte de los hallazgos relevantes en la investigación (véase la tabla 6.29).

Tabla 6.29 Información sobre el hallazgo “software”.

Identificador del hallazgo	ANA-HED-10
Identificador del dispositivo origen	PC-02-D01
Identificador del artefacto forense origen	IMGF-PC-02-DD01
Identificador del dispositivo usado para almacenar la evidencia	LAB-DDE-01
Descripción	Componente del registro de Windows, identificado en el disco duro del sistema dos.
Nombre del archivo	software
Ubicación del archivo	C:\windows\system32\config\
Hash MD5	c349ad02955904a4c80c4b9b170ceeeb

Existe una aplicación desarrollada por AccesData, misma empresa que desarrolla la aplicación FTK Imager, llamada Registry Viewer que permite la interpretación del contenido del archivo “software” en modo de solo lectura. Al ejecutar la aplicación, se indica la ruta del archivo (véase la figura 6.38) que contiene los valores del registro a analizar y la aplicación interpreta el contenido mostrándolo en una interfaz similar al utilizado por la aplicación “Editor de Registro” de Windows.

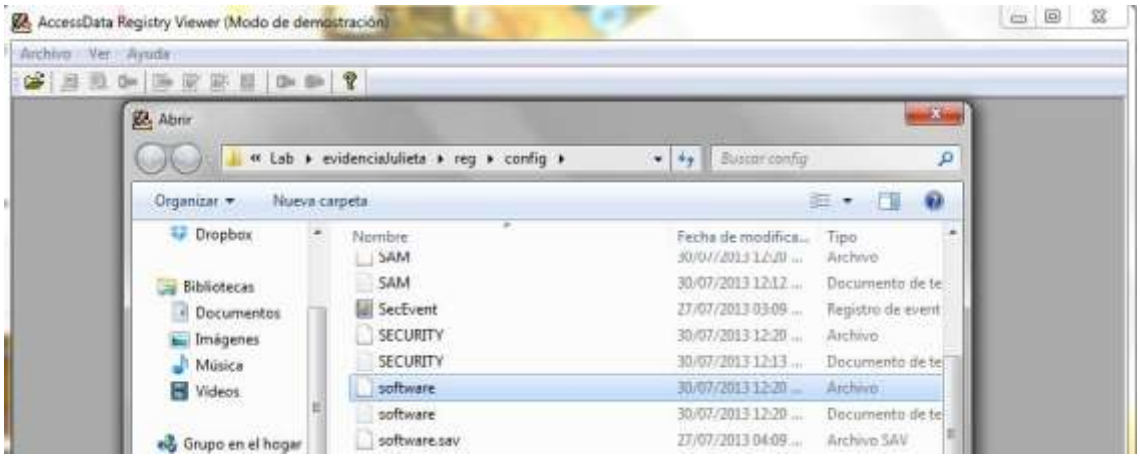


Figura 6.38 Selección del archivo “software” para la aplicación “Registry Viewer”.

Una vez que la aplicación ha leído e interpretado el contenido del archivo, basta con navegar en el árbol de directorios mostrado en la parte izquierda de la aplicación para consultar el valor de la llave de registro ubicada en: “SOTWARE\Microsoft\Windows\CurrenteVersion\Policies\Explorer\Run” (véase la figura 6.39) y determinar si el malware añadió el valor correspondiente para ejecutar la puerta trasera en cada inicio del sistema.

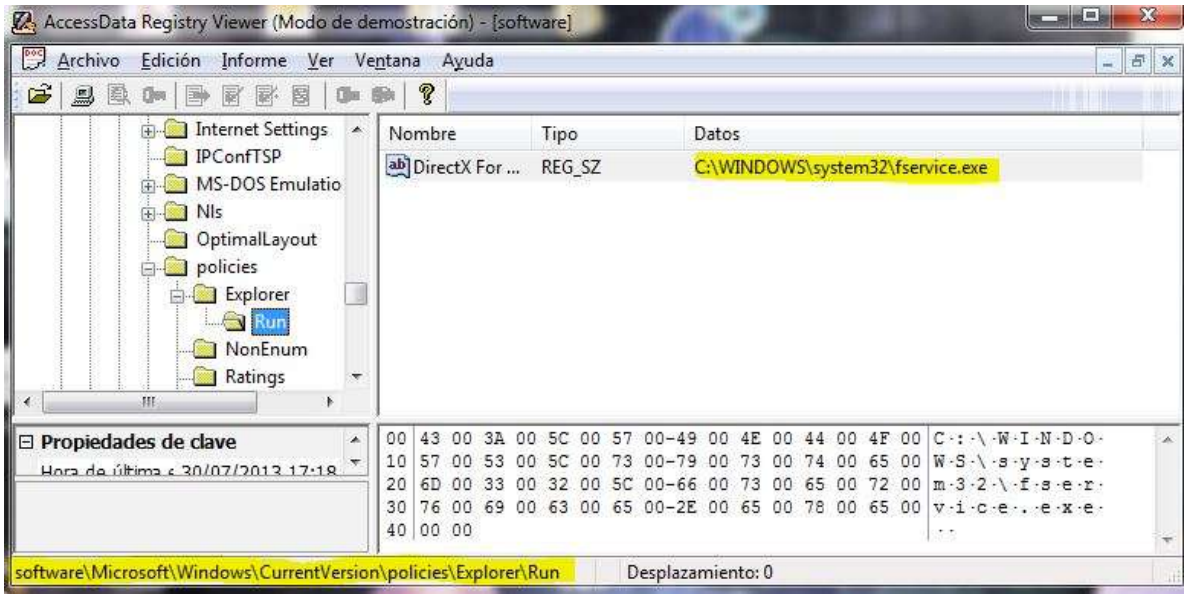


Figura 6.39 Entrada en el registro para la ejecución de “fservice.exe”.

Dentro de la llave de registro se identifica la variable “DirecX For Microsoft Windows” que contiene la ruta al programa malicioso “fservices.exe” para

ejecutarlo en cada inicio del sistema. Este dato representa un hallazgo muy importante para la investigación y debe ser documentado de manera individual a pesar que ya se documentó el archivo que lo contiene. La información correspondiente al hallazgo se documenta en la siguiente tabla (véase la tabla 6.29)

Tabla 6.30 Información sobre el hallazgo ANA-HED-11.

Identificador del hallazgo	ANA-HED-11
Identificador del dispositivo origen	PC-02-D01
Identificador del artefacto forense origen	IMGF-PC-02-DD01
Identificador del contenedor de hallazgos	LAB-DDE-01
Descripción del hallazgo	Variable “DirecX For Microsoft Windows” en la llave de registro HKLM\SOTWARE\Microsoft\Windows\CurrenteVersion\Policies\Explorer\Run para la ejecución al arranque del sistema de aplicación maliciosa (con identificador ANA-HED-06).
Nombre del archivo que contiene el hallazgo	software
Ubicación del archivo que contiene el hallazgo	C:\windows\system32\config\
Hash MD5 del archivo que contiene el hallazgo	c349ad02955904a4c80c4b9b170ceeeb

La información recolectada hasta el momento indica en el equipo de Julieta Guerrero también está infectado con el mismo software malicioso que se encontró en el equipo PC-01, por lo que es posible que la fuga de información se haya

perpetrado desde su estación de trabajo. Por tal motivo es necesario determinar cómo llego el malware al equipo.

Debido a que se trata del mismo software malicioso en ambos casos, es muy probable que la vía de infección sea la misma, por tanto es necesario revisar el historial de navegación del usuario buscando rastros de la descarga del archivo malicioso.

Según el cuestionario utilizado en la entrevista con el usuario del equipo, es necesario buscar el historial del navegador Google Chrome. De acuerdo con documentación del instituto SANS[34] el historial de navegación se ubica en "*C:\Documents and Settings\Adminstrador\Local Settings\Application Data\Google\Chrome\User Data\Default\".*

La figura 6.41 muestra que el archivo en cuestión se encuentra en la ubicación indicada dentro de la imagen forense capturada.

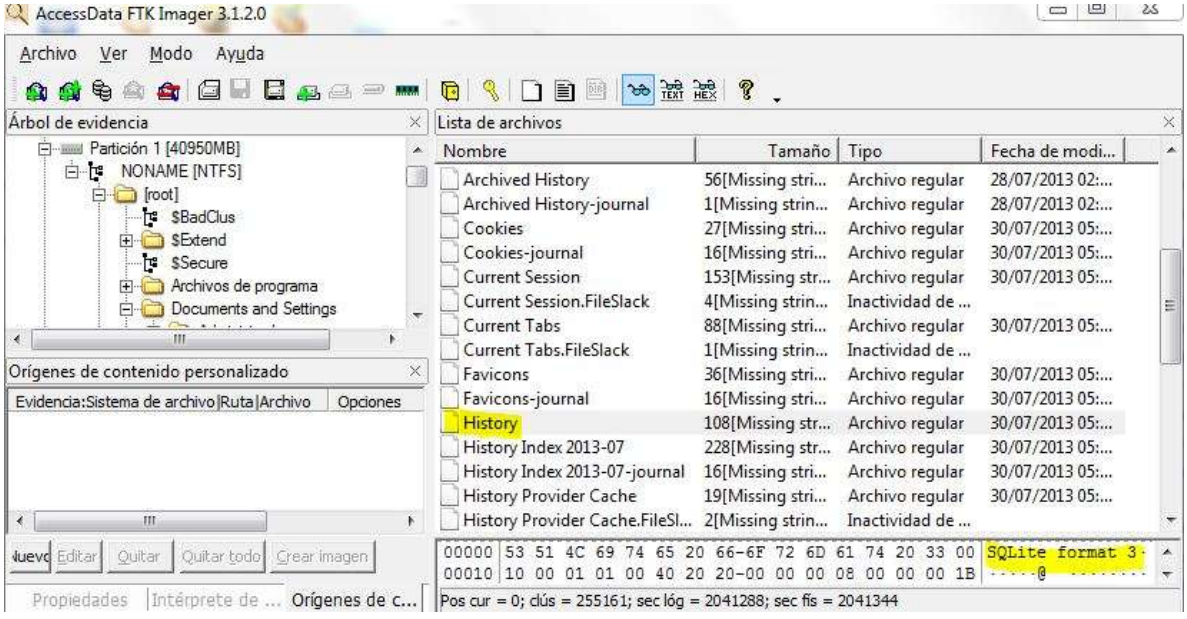


Figura 6.40 Ubicación del archivo "History.sqlite" en la imagen forense.

http://computer-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/

Una vez identificado es necesario extraer el archivo y documentar el hallazgo. La información relacionada se muestra en la tabla 6.30

Tabla 6.31 Documentación del hallazgo del archivo “History.sqlite”.

Identificador del hallazgo	ANA-HED-12
Identificador del dispositivo origen	PC-02-D01
Identificador del artefacto forense origen	IMGF-PC-02-DD01
Identificador del contenedor de hallazgos	LAB-DDE-01
Descripción	Archivo que contiene el historial de navegación de la cuenta de usuario “Administrador” para Google Chrome.
Nombre del archivo	History.sqlite
Ubicación del archivo	C:\Documents and Settings\Administrador\Local Settings\Application Data\Google\Chrome\
Hash MD5	1072f5cee0640caaefa48843eda6614c

El archivo “History” es una base de datos que contiene toda la información de navegación realizada por el usuario. El siguiente paso es analizar el contenido de la base de datos a través de consultas[35]. Existen aplicaciones que permiten realizar consultas básicas mediante una interfaz gráfica. La aplicación **SQLiteManager** ofrece este tipo de interfaz (Véase la figura 6.41).

[35] Guía de referencia: http://computer-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/

Figura 6.41 Consulta de las descargas realizadas.

La consulta muestra que se descargaron los archivos "wrar420es.exe" y "descuentosCam.rar" al directorio predeterminado para las descargas en los sistemas Microsoft Windows XP. La figura 6.42 muestra los archivos correspondientes en la imagen forense.

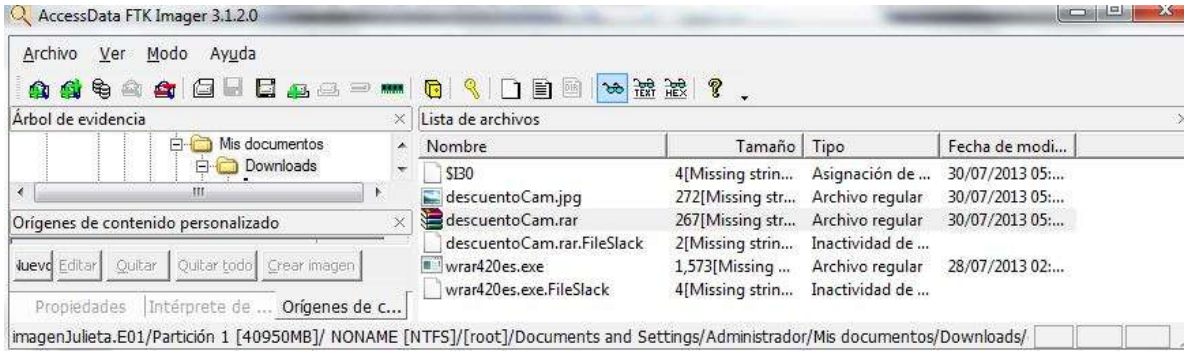


Figura 6.42 Contenido de la carpeta predeterminada de descargas.

Para comprobar que se trata de los mismos archivos, se extraen de la imagen forense y se documentan. Los valores del Hash md5 de ambos archivos son los mismos que los valores de los archivos encontrados en el equipo PC-01. La tabla 6.31y 6.32 muestra la información relacionada a los hallazgos de los archivos "descuentosCam.rar" y "descuentosCam.exe" respectivamente.

Tabla 6.32 Información del hallazgo del archivo "descuentosCam.rar".

Identificador de archivo	ANA-HED-13
Identificador del dispositivo origen	PC-02-D01
Identificador del artefacto forense origen	IMGF-PC-02-DD01
Identificador del contenedor de	LAB-DDE-01

hallazgos	
Descripción	Archivo comprimido descargado a través de Google Chrome, contiene la aplicación maliciosa.
Nombre	descuentosCam.rar
Ubicación	C:\Documents and Settings\Administrador\ Mis documentos\Descargas\
Hash MD5	070f6618a9500eef793984283621feaa
Última fecha de modificación	30/07/2013

Tabla 6.33 Información sobre el hallazgo del archivo “descuentosCam.exe”.

Identificador del archivo	ANA-HED-14
Identificador del dispositivo origen	PC-02-D01
Identificador del artefacto forense origen	IMGF-PC-02-DD01
Identificador del contenedor de hallazgos	LAB-DDE-01
Descripción	Aplicación maliciosa identificada previamente en el sistema uno, ejecutada también en el sistema dos.
Nombre del archivo	descuentosCam.exe
Ubicación del archivo	C:\Documents and Settings\Administrador\ Mis documentos\Descargas\
Hash MD5	1072f5cee0640caaefa48843eda6614c
Última fecha de modificación	30/07/2013

La ventaja de realizar consultas directamente a la base de datos es que es posible obtener la información de interés según la consulta realizada. Sin embargo no es la única opción para obtener información sobre el historial de navegación, la

aplicación ChromeAnalysis[36] es capaz de interpretar los datos del historial y presentar la información de manera detallada sin tener que realizar consultas manualmente, lo que resulta en un ahorro de tiempo al realizar la investigación.

Para utilizar esta aplicación es necesario recuperar todos los archivos alojados en la ubicación: "C:\Documents and Settings\Adminstrador\Local Settings\Application Data\Google\Chrome\User Data\Default\" con la intención de que la herramienta tenga acceso a toda la información necesaria para desplegarla dentro de su interfaz. Después de haber extraído los datos de la imagen forense se ejecuta la aplicación ChromeAnalysis indicando la ruta en la que se encuentran los archivos (véase la figura 6.43).

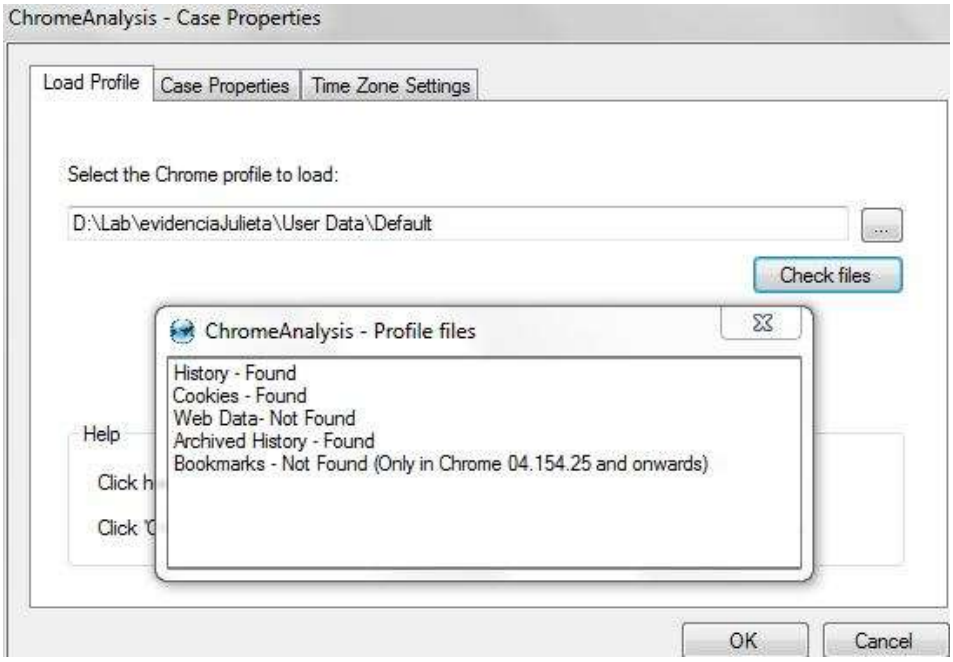


Figura 6.43 Herramienta ChromeAnalysis.

La figura 6.44 muestra la interfaz de la aplicación después de procesar los datos del historial, es posible identificar la línea correspondiente a la visualización del correo malicioso que llegó a la cuenta "contacto.sviw@gmail.com" (véase la figura 6.44).

[36]http://forensic-software.co.uk/

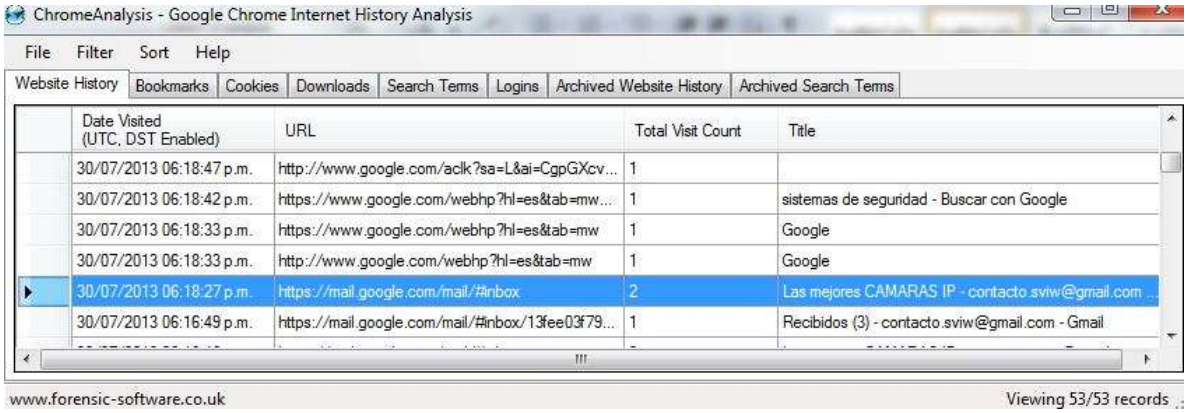


Figura 6.44 Visualización del correo malicioso.

Con estos elementos de información es posible asegurar que el usuario, Julieta Guerrero, visualizó el correo malicioso en su equipo y descargó el archivo adjunto "descuentoCam.rar" y lo descomprimió. De esta forma se esclarece el cómo llegó el malware al equipo. Sin embargo, debido al borrado del correo original con el archivo adjunto no es posible identificar la procedencia del mismo.

6.11. Etapa de presentación.

Esta etapa contempla la presentación de los resultados obtenidos al finalizar la investigación. Incluye los procedimientos técnicos más relevantes, resultados y la interpretación de los mismos.

La presentación de los resultados de la investigación incluye:

- Antecedentes
- Informe ejecutivo
- Actividades realizadas
    - Análisis de procesos en ejecución en el sistema del equipo PC-01
    - Análisis de conexiones de red en el sistema del equipo PC-01

    - Volcado y análisis de la memoria RAM del sistema del equipo PC-01
    - Análisis básico de malware
    - Generación de imagen forense del equipo PC-01
    - Identificación de archivos maliciosos en el equipo PC-01
    - Análisis del historial de navegación en Internet del equipo PC-01
    - Generación de imagen forense del equipo PC-02
    - Identificación de archivos maliciosos en el equipo PC-02
    - Análisis del historial de navegación en Internet del equipo PC-02
- Conclusiones
- Recomendaciones

6.11.1 Antecedentes.

El día 21 de agosto de 2013 la Ing. Julieta Guerrero, Directora General de la empresa Vigilancia y Seguridad IW, ha solicitado una investigación basada en cómputo forense para identificar al responsable de la fuga de información confidencial relacionada a propuestas para el desarrollo de diferentes proyectos relacionados con sistemas de seguridad.

La Ing. Guerrero sospecha de su empleado, Ing. Salvador Pedrosa, y solicita revisar su equipo para identificar actividad relacionada con la posible fuga de información, al inicio de la investigación el equipo se encontró encendido y con una sesión iniciada, por tal motivo se realizó la recopilación de información volátil dando comienzo a la investigación.

6.11.2 Informe ejecutivo.

Debido a la falta de información no es posible asegurar que la fuga de información confidencial sea producto de actividad realizada por el Ing. Salvador Pedrosa.

Los equipos que almacenan la información confidencial se encuentran infectados con un programa malicioso que permite a un intruso acceder y controlar dichos sistemas de forma encubierta, así como descargar archivos del equipo.

Los equipos se infectaron después de ejecutar un programa malicioso que llegó como archivo adjunto en un mensaje a la cuenta de correo "contacto.sviw@gmail.com".

El mensaje fue visualizado por el Ing. Pedrosa el día 17 de julio de 2013, mismo día que el programa malicioso fue ejecutado en el sistema. La Ing. Guerrero visualizó el mensaje y ejecutó el programa el día 30 de julio de 2013. Ambos comparten las credenciales de esa cuenta de correo. El mensaje fue eliminado, por lo tanto no es posible determinar su origen.

6.11.3 Actividades realizadas.

La investigación fue realizada por Demian García, y toda la documentación correspondiente se encuentra en el expediente Caso B-201306-SVIW. A continuación se detallan las actividades realizadas.

6.11.3.1 Análisis de procesos en ejecución en el sistema del equipo PC-01

Se listaron los procesos a través de la herramienta Process Explorer de Sysinternals y se identificó un proceso sospechoso, "services.exe" con PID 456, sin información en los campos correspondientes a la descripción del proceso y el nombre de la compañía que lo desarrolla, tampoco fue posible identificar la ubicación del ejecutable ni identificar las cadenas imprimibles embebidas en el archivo.

6.11.3.2 Análisis de conexiones de red en el sistema del equipo PC-01

Se identificaron conexiones de red establecidas con un equipo remoto desconocido[37], también se identificaron puertos a la escucha de nuevas conexiones, tanto las conexiones como los puertos fueron levantados por el proceso sospechoso "services.exe", la información se muestra en la tabla 6.23

Tabla 6.34 Información sobre conexiones de red del proceso sospechoso.

Identificador del hallazgo			ANA-HED-01	
Identificador del dispositivo origen			PC-01	
Descripción			Información sobre conexiones de red relacionadas con un proceso sospechoso, obtenidas mediante la herramienta TCPView.	
Nombre del proceso			Services.exe	
PID			456	
Puerto local	Host remoto	Puerto remoto	Protocolo	Estado de la conexión
5112	Master-ea14e6ab	1159	TCP	Establecida
51100	Master-ea14e6ab	1162	TCP	Establecida
51100	Master-ea14e6ab	1179	TCP	Establecida
5110	Master-ea14e6ab	1158	TCP	Establecida
51100	Master-ea14e6ab	1160	TCP	Establecida
51100	Master-	1164	TCP	Establecida

[37] El equipo remoto tiene asignada una dirección IP privada, en un caso real, la IP que participa en la comunicación es de tipo pública y debe investigarse a nombre de quien está registrada, para dicho propósito puede usarse el servicio whois o consultar un sitio como http://whois.domaintools.com

	ea14e6ab			
5112	localhost	0	TCP	A la escucha
51100	localhost	0	TCP	A la escucha
5110	localhost	0	TCP	A la escucha

6.11.3.3 Volcado y análisis de la memoria RAM del sistema del equipo PC-01

Se realizó un volcado de la información en memoria RAM, el procedimiento fue documentado en el formato PRE-GVM-01 (véase la tabla 6.33).

Tabla 6.35 Información referente a la generación del volcado de memoria.

Formato: PRE-GVM-01	
Identificadores	
Identificador del volcado de memoria	MDUMP-PC-01-RAM01
Identificador del dispositivo origen	PC-01-RAM01
Identificador de la cadena de custodia a la que pertenece el dispositivo	CC-01
Identificador del dispositivo donde se aloja el volcado de memoria	LAB-DDE-01
Información de la generación de la imagen	
Herramienta usada	DumpIt
MD5 de la herramienta	84f0feb07beae896d471f45527d781b0
Identificador del dispositivo donde se aloja la imagen	ED-001
Nombre del archivo generado	memDump.bin
MD5 de la imagen generada	ef6a7ab2afb99dfdb3218f9d35998130
Formato de la imagen	.bin
Tamaño de la imagen	512MB
Responsable de la generación del a imagen	Demian García

Firma del responsable	
Hora y fecha de la generación	21 agosto 2013, 17:00hrs
Identificado de la bitácora de hashes	HASH- PC-001-RAM001

Al analizar la información alojada en memoria se identificaron dos aplicaciones maliciosas en el sistema, la primera se trata de las instrucciones ejecutadas por el proceso “services.exe”, cargadas en la memoria RAM y volcadas a un archivo ejecutable. El archivo generado se identifica como el hallazgo: ANA-HED-02. Al analizar el archivo con el servicio de Virus Total se identifica que se trata de una aplicación maliciosa como se muestra en la figura 6.45

Figura 6.45 Resultado del análisis del hallazgo ANA-HED-02.

La segunda aplicación maliciosa identificada en el sistema es el archivo “descuentoCam.exe” que se identificó dentro del archivo comprimido “C:\Documents and Settings\Administrador\ Mis documentos\Descargas\ descuentoCam.rar”. A este archivo ejecutable se le asigna el identificador de hallazgo ANA-HED-04, y el análisis en Virus Total indica que se trata de un troyano ProRAT (véase la figura 6.46).

Figura 6.46 Resultado del análisis del hallazgo ANA-HED-03.

6.11.3.4 Análisis básico de malware.

Debido a las características del malware, la capacidad de conectarse remotamente al equipo infectado y tomar control del sistema, es necesario analizar el archivo “descuentoCam.exe” en un ambiente controlado.

El resultado del análisis indica que al ejecutar la aplicación maliciosa se despliega una imagen que muestra diferentes tipos de cámaras mientras se copia el archivo fservice.exe en el directorio C:\Windows\system32\, se modifica la llave de registro HKLM\SOTWARE\Microsoft\Windows\CurrenteVersion\Policies\Explorer\Run agregando la variable “DirecX For Microsoft Windows” para asegurar que el programa “fservice.exe” se ejecute en cada inicio del sistema. Este programa es responsable de levantar el proceso “services.exe” encargado de levantar los puertos 5112, 51100, 5110 a la espera de conexiones entrantes.

6.11.3.5 Generación de imagen forense del equipo PC-01.

Es necesario determinar cómo llegó el malware al equipo, por tal motivo se realiza una imagen forense del disco duro con identificador PC-01-DD01. El procedimiento se documenta en el formato PRE-GIF-01 (véase la tabla 6.34).

Tabla 6.36 Información referente a la generación de la imagen forense.

Formato: PRE-GIF-01	
Identificadores	
Identificador de la imagen forense	IMGF-PC-01-DD01
Identificador del dispositivo origen	PC-01-DD01
Identificador de la cadena de custodia a la que pertenece el dispositivo	CC-001
Identificador del dispositivo usado para almacenar la imagen	LAB-DDE-01
Información de la generación de la imagen	
Herramienta usada	FTK Imager
MD5 de la herramienta	f6d2c8f47461e589410a17c097c29385
MD5 de la imagen generada	ef6a7ab2afb99dfdb3218f9d35998130
Formato de la imagen	.E01
Tamaño de la imagen	81GB
Responsable de la generación del a imagen	Demian García
Firma del responsable	
Hora y fecha de la generación	21 agosto 2013, 21:00hrs
Identificado de la bitácora de hashes	HASH-PC-009-DD001

6.11.3.6 Identificación de archivos maliciosos en el equipo PC-01.

En la imagen forense se identificó el archivo malicioso “fservices.exe” (véase la figra 6.47), el identificador ANA-HED-06 fue asignado a este hallazgo. Al comparar el valor del hash MD5 de este hallazgo con el hash MD5 del archivo “fservices.exe” identificado en el análisis de malware se puede concluir que es la misma aplicación maliciosa.

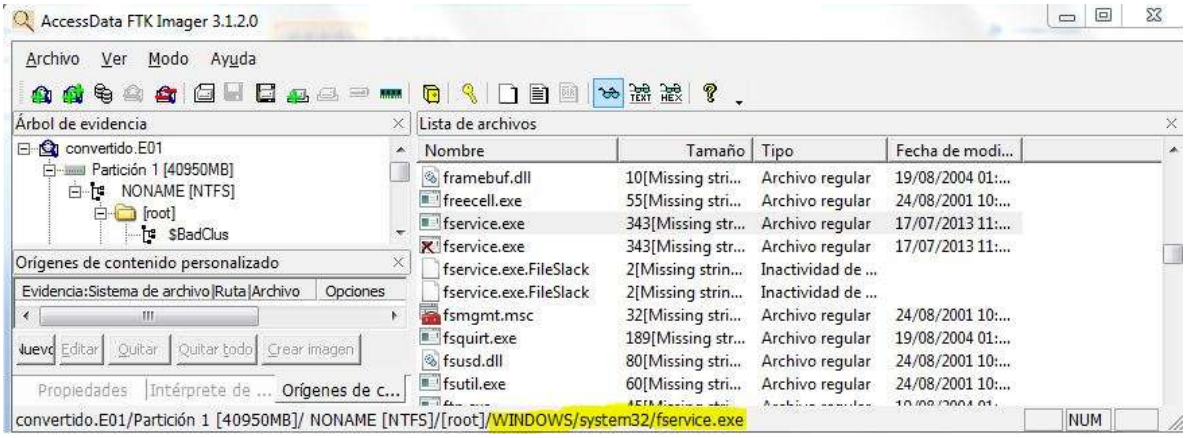


Figura 6.47 Archivo fservice.exe en el disco duro del sistema uno.

6.11.3.7 Análisis del historial de navegación en Internet del equipo PC-01.

Se identificó el archivo “places.sqlite” en la imagen forense (véase la figura 6.48), para este hallazgo se asignó el identificador ANA-HED-07, el archivo en cuestión se extrajo de la imagen forense para su análisis en la estación de investigación.

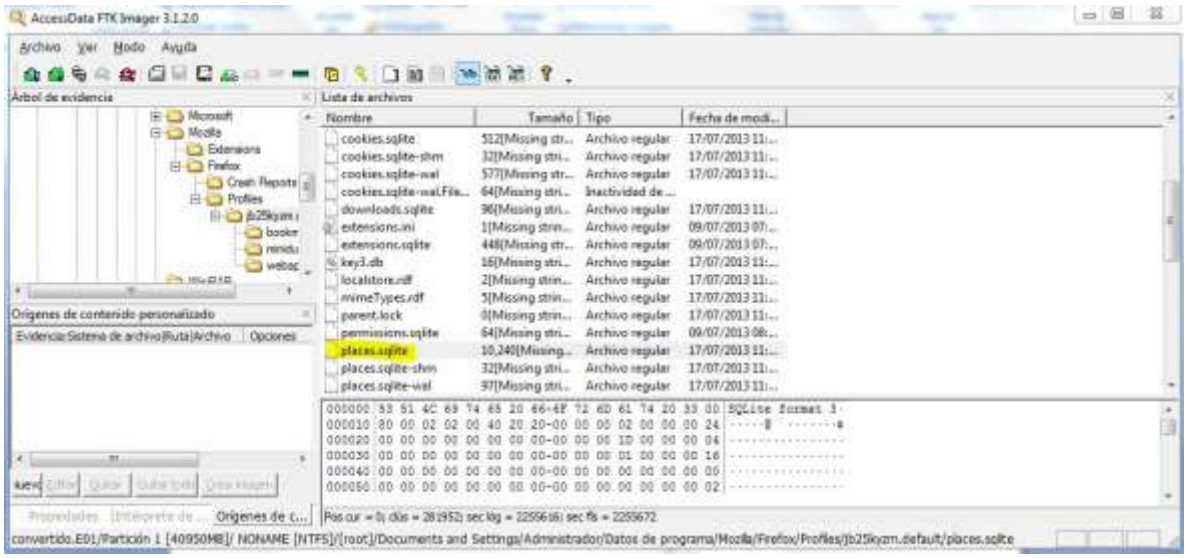


Figura 6.48 Ubicación del archivo “places.sqlite” en la imagen forense.

Al analizar el archivo que contiene el historial de navegación del explorador Mozilla Firefox se determinó que el archivo “descuentoCam.rar” es un archivo adjunto que llegó a la cuenta de correo contacto.sviw@gmail.com y fue descargado al equipo el día 17 de julio de 2013 (véase la figura 6.49).

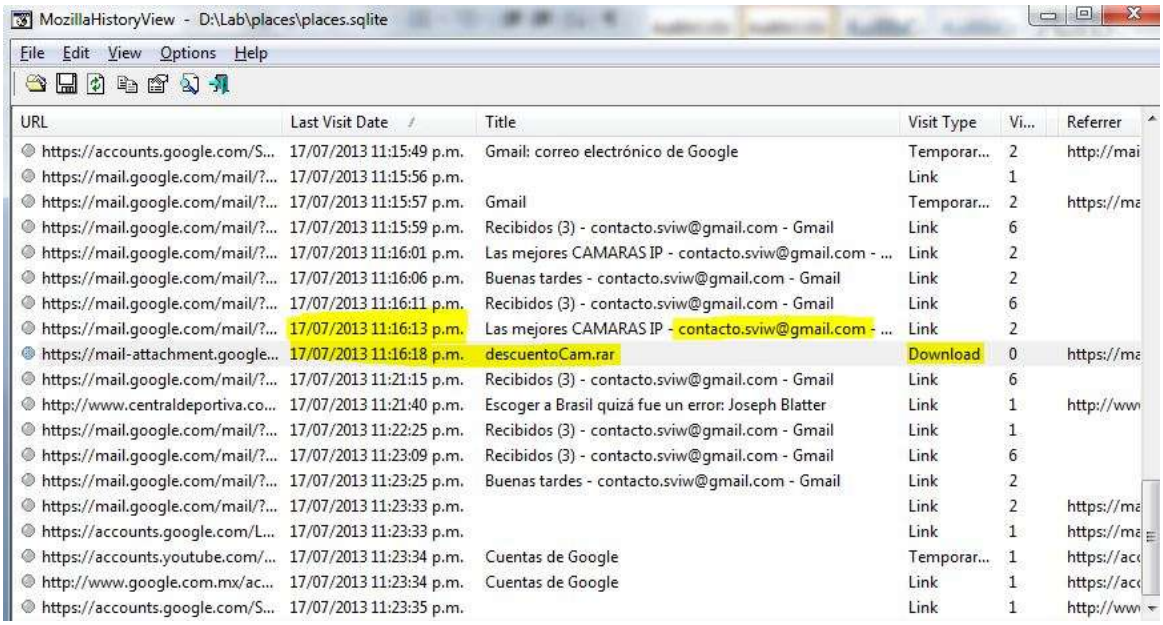


Figura 6.49 Descarga del archivo “descuentoCam.rar”.

Se identificó que ese mismo día se descomprimió el archivo descargado, el cual contiene la aplicación maliciosa “descuentoCam.exe”, hallazgo al que se le asignó el identificador ANA-HED-08.

No fue posible identificar la procedencia del correo con archivo adjunto malicioso debido a que la Ing. Guerrero eliminó el correo de manera permanente.

6.11.3.8 Generación de imagen forense del equipo PC-02.

Se analizo el sistema utilizado por la Ing. Guerrero debido al uso compartido de la cuenta de correo "contacto.sviw@gmail.com" con el objetivo de determinar si el equipo se encuentra infectado por el mismo malware. El procedimiento de generación de la imagen forense se documenta en el formato PRE-GIF-02 (véase la tabla 6.35)

Tabla 6.37 Información referente a la generación de la imagen forense.

Formato: PRE-GIF-02	
Identificadores	
Identificador de la imagen forense	IMGF-PC-02-DD01
Identificador del dispositivo origen	PC-02-DD02
Identificador de la cadena de custodia a la que pertenece el dispositivo	CC-002
Identificador del dispositivo donde se aloja la imagen	LAB-DDE-01
Información de la generación de la imagen	
Herramienta usada	FTK Imager
MD5 de la herramienta	f6d2c8f47461e589410a17c097c29385
MD5 de la imagen generada	b1d7861bb4090b3ee2b5b4501d1f22f8
Formato de la imagen	.E01
Tamaño de la imagen	81GB
Responsable de la generación del a imagen	Demian García
Firma del responsable	
Hora y fecha de la generación	22/08/2013, 12:49hrs

Identificado de la bitácora de hashes	HASH-PC-02-DD01

6.11.3.9 Identificación de archivos maliciosos en el equipo PC-02.

Se identificó el archivo “fservice.exe” en el disco duro del equipo PC-02 (véase la figura 6.50) en la misma ubicación en el sistema anterior y en el análisis de malware.

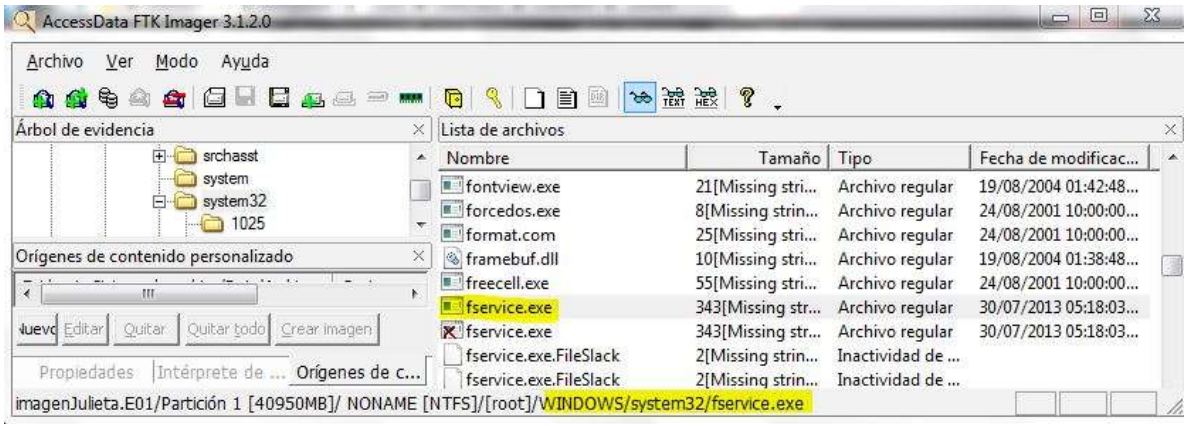


Figura 6.50 Ubicación del malware “fservice.exe”.

A este hallazgo se le asignó el identificador ANA-HED-09 y se documentó el valor del hash MD5, mismo valor que el obtenido para el mismo archivo encontrado en los sistemas antes analizados.

Se identificó la misma modificación a la llave de registro “HKLM\SOTWARE\Microsoft\Windows\CurrenteVersion\Policies\Explorer\Run” en este sistema como en el sistema usado para el análisis de malware. Se comprobó que la aplicación maliciosa se ejecuta cada vez que se inicia el sistema (véase la figura 6.51).

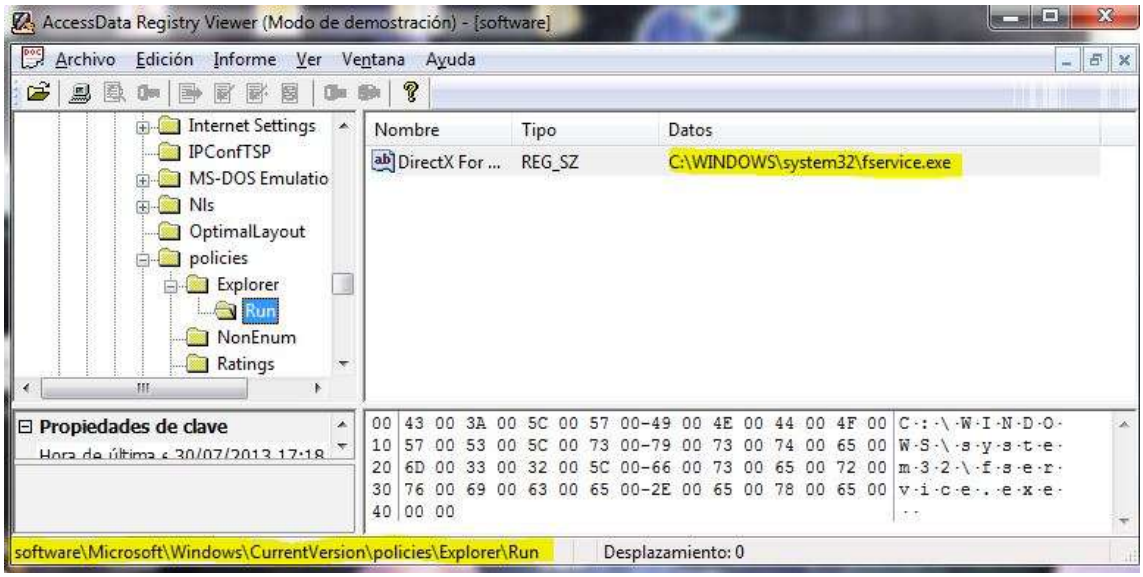


Figura 6.51 Entrada en el registro para la ejecución de “fservice.exe”.

A este hallazgo se le asignó el identificador ANA-HED-11.

6.11.3.10 Análisis del historial de navegación en Internet del equipo PC-02.

Se identificó el archivo “History.sqlite” en la imagen forense (véase la figura 6.52), para este hallazgo se asignó el identificador ANA-HED-12, el archivo en cuestión se extrajo de la imagen forense para su análisis en la estación de investigación.

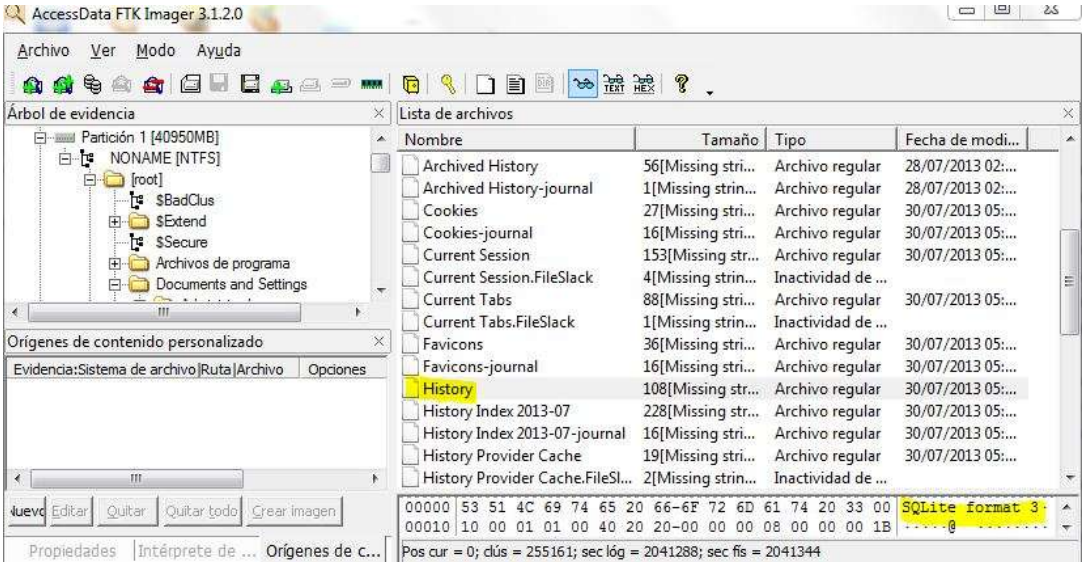


Figura 6.52 Ubicación del archivo “History.sqlite” en la imagen forense.

Al analizar el archivo que contiene el historial de navegación del explorador Google Chrome se determinó que el archivo “descuentoCam.rar” fue descargado al equipo el día 30 de julio de 2013 y el correo con asunto “Las mejores CAMARAS IP” enviado a la cuenta “contacto.sviw@gmail.com” fue visualizado ese mismo día (véase la figura 6.53).

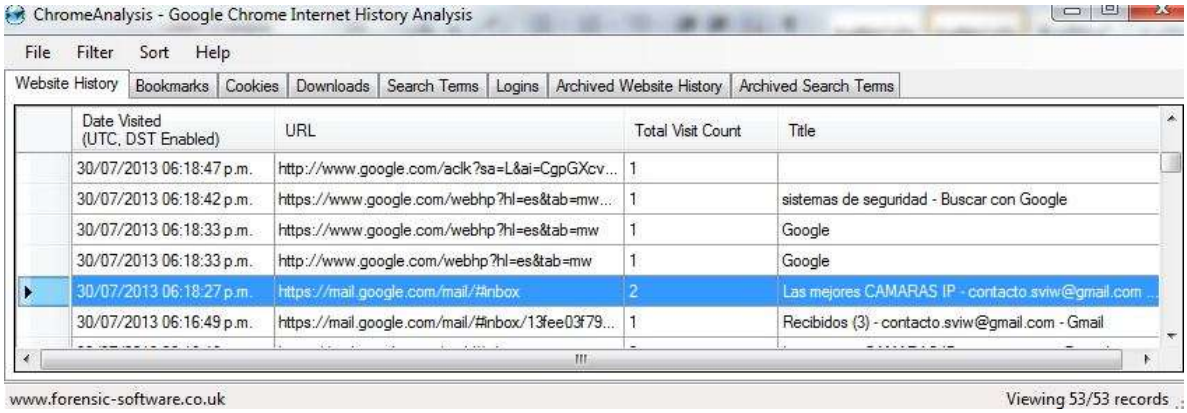


Figura 6.53 Visualización del correo malicioso.

Se identificó que ese mismo día se descomprimió el archivo descargado, el cual contiene la aplicación maliciosa “descuentoCam.exe”, hallazgo al que se le asignó el identificador ANA-HED-14.

No fue posible identificar la procedencia del correo con archivo adjunto malicioso debido a que la Ing. Guerrero eliminó el correo de manera permanente.

6.11.4 Conclusiones.

Debido a la falta de información no es posible asegurar que la fuga de información confidencial sea producto de actividad realizada por el Ing. Salvador Pedrosa.

Los equipos que almacenan la información confidencial se encuentran infectados con un programa malicioso que permiten a un intruso acceder y controlar dichos sistemas de forma remota, entre las acciones que puede realizar se encuentran la

carga y descarga de archivos desde y hacia los equipos infectados, modificaciones en las configuraciones del equipo, entre otras.

Los equipos se infectaron después de ejecutar un programa malicioso, descuantoCam.exe, que llegó como adjunto en un archivo comprimido, descuentosCam.rar, en un mensaje con asunto “Las mejores CAMARAS IP” enviado a la cuenta de correo “contacto.sviw@gmail.com”.

El mensaje fue visualizado por el Ing. Pedrosa el día 17 de julio de 2013, mismo día que el programa malicioso fue ejecutado en el sistema. La Ing. Guerrero visualizó el mensaje y ejecutó el programa el día 30 de julio de 2013. Ambos comparten las credenciales de esa cuenta de correo.

El correo malicioso fue eliminado de la cuenta de correo y no es posible recuperarlo para su análisis.

Debido a la falta de evidencia no es posible identificar el uso de algún otro mecanismo para la extracción de la información confidencial.

6.11.5 Recomendaciones.

- Instalar un sistema antivirus actualizado y desinfectar las estaciones de trabajo.
- Establecer políticas de actualización automática del software antivirus.
- Instalar y configurar un firewall que controle y registre las comunicaciones entre las estaciones de trabajo e Internet.
- Establecer políticas para el uso, manejo y almacenamiento de los datos relacionados a cada proyecto.
- Implementar sistemas de cifrado para las estaciones de trabajo, por ejemplo, cifrado de Windows o aplicaciones comerciales como TrueCrypt.
- Configurar el reenvío automático de mensajes entrantes de la cuenta “contacto.sviw@gmail.com” para que estos lleguen a las cuentas

personales de los Ing. Guerrero y Pedrosa, con el objetivo de almacenar copias de todos los mensajes enviados a la cuenta compartida.

- Configurar filtros anti SPAM en las cuentas de correo usados por todo el personal de la empresa.
- Establecer políticas de uso de los equipo de cómputo pertenecientes a la empresa.
- Implementar acuerdos de confidencialidad con todas las personas que manejen información sensible.
- Realizar campañas de concientización de seguridad de la información entre los empleados de la empresa.
- Cambiar el sistema operativo de las estaciones de trabajo que utilicen Windows XP por un sistema operativo que cuente con soporte para actualizaciones de seguridad a mediano y largo plazo.

Implementar políticas de contraseñas seguras para las estaciones de trabajo y cuentas de correo electrónico.

Conclusiones

El trabajo aquí presentado cumple con los objetivos planteados al inicio de la investigación. Se consiguió desarrollar una metodología de fácil acceso para la investigación de incidentes de seguridad informática, mismos que, de acuerdo a su contexto, pueden ser considerados cómo delitos informáticos.

La metodología desarrollada ofrece una guía clara y precisa para realizar una investigación basada en cómputo forense, a pesar de que cada investigación es diferente, la forma estructurada de la metodología provee bases sólidas para llevar a cabo cualquier investigación ya que contempla las principales etapas del cómputo forense además de incluir el análisis básico de malware para complementar la metodología.

La aplicación de la metodología en la investigación de incidentes de seguridad en ambientes controlados sirve como muestra del alcance y resultados que ofrece esta herramienta, además de ofrecer una guía para las personas interesadas en utilizar esta metodología en sus investigaciones.

La documentación de los procedimientos realizados en las investigaciones de los casos A y B muestran los beneficios de aplicar esta metodología. Toda la información generada en cada investigación se encuentra debidamente ordenada según la etapa correspondiente a una investigación en cómputo forense y provee de recursos documentales que validan la veracidad de la información y resultados generados.

Particularmente, en el Caso A, los resultados obtenidos son favorables ya que se identificó al responsable de la fuga de información después de realizar los procedimientos planteados en la metodología. Durante la fase de identificación se aplicó una serie de preguntas cuyas respuestas encaminaron el curso de la investigación.

La fase de preservación se desarrolló como está contemplado en la metodología para un sistema detenido, procedimiento que generó material adecuado para su análisis, mismo que concluyó con la identificación del mecanismo de extracción de información confidencial y la cuenta de usuario involucrada en dicha actividad.

En contraparte, los resultados de la investigación del Caso B resultaron inconclusos, debido a la falta de información en los sistemas analizados. Durante la investigación se realizaron los procedimientos correspondientes al análisis en vivo, mismos que incluyen, por mencionar algunos, la preservación y análisis de información volátil. En esta investigación también se realizó un análisis básico de malware, cuyos resultados apuntaron a la relación de una pieza de malware con la fuga de información confidencial.

La investigación continuó con el análisis de dos sistemas detenidos y se determinó que ambos sistemas se encontraban infectados con la misma pieza de malware, misma que permite la conexión al equipo de manera remota eludiendo los mecanismos de autenticación del sistema operativo. La metodología condujo a identificar el momento de la infección, mismo que corresponde a la ejecución de una aplicación adjunta a un correo electrónico. Sin embargo no fue posible determinar el origen del correo debido a que fue eliminado antes de iniciar la investigación.

Este tipo de escenario, donde no se cuenta con la información necesaria para responder todas las preguntas que plantea una investigación, es bastante común en el mundo laboral, causado por la falta de protocolos para responder a incidentes de seguridad o la mala aplicación de los mismos. También es causado por falta de educación por parte de las personas respecto a seguridad de la información.

Para estos casos, la metodología ofrece una guía bastante competitiva que resulta de utilidad para identificar fallas u oportunidades de mejora en los protocolos de respuesta a incidentes, lo que se traduce en una mejora en la seguridad de la información de las empresas a través de la atención a dichas oportunidades de mejora.

Una ventaja adicional de la metodología desarrollada es su independencia tecnológica, su uso no requiere de alguna herramienta comercial o dispositivo para la correcta implementación de la metodología en una investigación, característica

que reduce el costo que las empresas deben invertir para investigar un incidente de seguridad implementando el enfoque del cómputo forense.

Las herramientas presentadas en el desarrollo de casos prácticos no requieren de la adquisición de alguna licencia para ser utilizadas, además de que su uso no es mandatorio para la implementación de la metodología. Cada investigador es libre de elegir el juego de herramientas y dispositivos que mejor se ajuste a sus necesidades y presupuesto.

Gracias a la independencia tecnológica, la metodología se mantiene accesible para todo tipo de personas interesadas en las investigaciones digitales, punto fundamental para las perspectivas a futuro de este trabajo de investigación ya que se pretende hacer llegar este trabajo al público en general a través de su difusión en Internet.

Una campaña de difusión conseguirá que las personas interesadas en respuesta a incidentes, cómputo forense, seguridad de la información, entre otros, conozcan la existencia de esta herramienta y la implementen en investigaciones de casos reales o controlados. Esta implementación contribuiría a identificar fallas o puntos a mejorar en cada fase de la metodología aquí propuesta, e idealmente, las personas que utilicen ésta herramienta proporcionarán retroalimentación sobre su experiencia con la metodología.

La retroalimentación permitirá mejorar y afinar los pasos necesarios e incluso generar nuevos procedimientos para su inclusión según corresponda. Toda la información será recibida en la cuenta de correo demian@comunidad.unam.mx, se espera contar con la colaboración de la comunidad para mantener la herramienta vigente y siempre disponible para cualquier persona.

Otra alternativa para probar la herramienta en casos reales es que algún estudiante de ingeniería interesado en desarrollar una tesis retome este trabajo y se encargue de implementar la metodología en investigaciones de casos en ambientes reales. Los resultados de esta actividad serían de gran ayuda para mejorar la herramienta, sin embargo es una tarea complicada debido al sitio que

ocupa la seguridad de la información en las prioridades de una PYME, y en particular la carencia de protocolos de respuesta a incidentes.

Hace falta mucho trabajo de difusión y concientización de temas de seguridad entre las empresas, entidades de gobierno y el público en general, hace falta gente especializada que se encargue de hacer esa difusión y que sea capaz de generar soluciones en materia de seguridad de la información para hacer frente a todas las amenazas a las que está expuesta la información de estos sujetos.

Con este trabajo de investigación se espera contribuir a la solución de problemas relacionados con la seguridad de la información a través de una herramienta diseñada para ser un apoyo en la investigación de delitos informáticos basada en cómputo forense, de fácil acceso y de libre distribución.

Anexo I

El Consejo de Europa y el Convenio sobre la Ciberdelincuencia

El Consejo de Europa es un organismo conformado por los jefes de Estado o de Gobierno de cada país de la Unión Europea (UE), el presidente de la Comisión y el Alto Representante para los Asuntos Exteriores y Política de Seguridad[38], éste organismo es presido por presidente del Consejo Europeo quien tiene un mandato de dos años y medio con posibilidad de una renovación.

Éste organismo tiene como propósito definir las prioridades políticas generales de la UE, sesiona dos veces por semestre, por lo general en Bruselas, y puede sesionar de manera extraordinaria en función de la situación. La toma de decisiones dentro del consejo es realizada a través un consenso, donde dependiendo del Tratado en cuestión es necesaria la mayoría cualificada o la unanimidad.

El Consejo Europeo fue formado en 1974 como un foro internacional de debate entre los jefes de estado, sin embargo se fue consolidando como un organismo trascendental para la UE ya que en este foro se comenzaron a fijar objetivos, y las acciones necesarias para alcanzarlos, para todos los ámbitos de actividad de la UE. De tal modo que en 1992 adquirió un estatuto oficial y para 2009 se convirtió en una de las siete organizaciones de la UE.

En 1976 aparece por primera vez dentro de la agenda del Consejo Europeo la preocupación por los delios informáticos y su naturaleza trasnacional y es en 1985 que se designa a un comité de expertos la tarea de analizar los aspectos jurídicos de los delitos informáticos, dicho comité estaba conformado por quince expertos de los 23 estados miembros y por observadores de Canadá, Japón, los Estados Unidos, la Comunidad Económica Europea, la Organización para la Cooperación del Desarrollo Económico, y Naciones Unidas[39].

A partir de la creación de ese grupo de trabajo las labores relacionadas con la lucha en contra del cibercrimen no se han detenido. En 1989 el Consejo Europeo adopta recomendaciones que son producto del Informe de Expertos sobre el delito

[38] http://www.european-council.europa.eu/the-institution?lang=es
[39] Information Technology Crime. Sieber. Ulrich. 1994. Pag. 577

cibernético[40]. Otras recomendaciones son adoptadas gracias al trabajo de comités dedicados al cibercrimen, hasta que el año de 1996 el Comité Europeo para Asuntos Delictivos decide establecer un nuevo comité de expertos con la encomienda de transformar todas las recomendaciones existentes en la redacción de un convenio internacional.

Uno de los puntos a resaltar en el trabajo de este nuevo comité es la cooperación de la UNESCO e Interpol[41], quienes a partir de sus acuerdos de cooperación para el combate contra la pedofilia y la pornografía infantil en Internet apoyaron a la elaboración del Convenio sobre la Ciberdelincuencia. Este convenio, una vez terminado y listo para su presentación, fue firmado en Budapest el 23 de noviembre de 2001 por 30 países incluidos cuatro Estados no miembros de la UE (Canadá, Estados Unidos, Japón y Sudáfrica).

Debido al trabajo realizado por el comité de expertos y el carácter internacional del convenio y la falta de material de referencia en la materia de delitos informáticos, éste convenio se ha convertido en un documento de referencia para muchos países. De acuerdo con la Unión Internacional de Telecomunicaciones (UIT), en su proyecto “El ciberdelito: Guía para los países en desarrollo” algunos países como Argentina, Pakistán, Filipinas, Egipto, Botswana y Nigeria, han redactado partes de su legislación basadas en el Convenio sobre la Ciberdelincuencia[42].

Sin embargo la falta de conocimiento en algunas naciones y los procesos burocráticos de otras han hecho que la adición a este convenio sea lenta. Para el año 2009 solo dieciséis nuevos Estados habían firmado en convenio dando un total de treintaiseises Estados firmantes de los cuales sólo veintiséis han ratificado el convenio[43]. El ritmo de firma y ratificación ha sido lento y más lento aun el de adición. Desde 2001 ningún país no miembro de la UE se ha adherido al convenio

[40] Information Technology Crime. Sieber. Ulrich. 1994. Pag. 576
[41] http://unesdoc.unesco.org/images/0011/001158/115849s.pdf
[42] El ciberdelito: Guía para los países en desarrollo. UIT. 2009. Pag. 104
[43] http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf

a pesar de que países como México, Costa Rica, Chile, República dominicana y Filipinas han sido invitados a hacerlo.

Cuando los organismos jurídicos legales de los países que no se han adherido al convenio o no lo han ratificado entiendan la seriedad del problema producido por la Ciberdelincuencia y realicen acciones para combatirla y cuando las naciones que han ratificado esta iniciativa comiencen a implementarla y a brindar las herramientas legales y la cooperación internacional para perseguir y castigar este tipo de delitos, será cuando estos esfuerzos rindan frutos en beneficio de la sociedad internacional.

Glosario

1. **Activo informático**: cualquier elemento de información que tenga un valor para una organización.
2. **Análisis forense**: rama de la computación dedicada a la aplicación de técnicas científicas y analíticas para la captura, procesamiento, análisis e investigación de información almacenada en computadoras utilizando una metodología donde la evidencia descubierta es aceptable en un proceso legal.
3. **Aplicaciones ofimáticas**: conjunto de aplicaciones, o programas, diseñados y ampliamente utilizados en ambientes de oficina, como los procesadores de texto, las hojas de cálculo, asistentes para hacer presentaciones, entre otras.
4. **Árbol de directorios**: representación gráfica del conjunto de directorios en una unidad de almacenamiento.
5. **Archivos *raw***: conjunto de datos sin procesar no poseen un formato en específico.
6. **Autoruns**: aplicación de Sysinternals que, entre otras cosas, permite listar los programas que se ejecutan al arranque de un sistema Windows.
7. **Cadena de custodia**: Procedimiento mediante el cual se busca garantizar la integridad de la evidencia digital mediante la documentación detallada de las interacciones y procesos a los que es sometida.
8. **Ciberbulling**: término utilizado para denominar la práctica de acoso, hostigamiento, humillación, abuso, entre otros, entre dos personas a través de Internet. Prácticas realizadas usualmente entre menores de edad.
9. **Ciberdelincuencia**: término utilizado para denominar prácticas delictivas que son realizadas con la ayuda de tecnologías de la información.
10. **Ciencias forenses**: conjunto de técnicas y procedimientos de investigación de los que está compuesta la criminalística.
11. **Cómputo forense**: equivalente de Análisis Forense.
12. **Contra informe**: documento que contiene los resultados de un segunda investigación de un caso y pretende refutar los resultados de una investigación en cómputo forense.
13. **Criminalística**: ciencia auxiliar del derecho penal encargada de describir, explicar y probar delitos que se encuentran bajo investigación.
14. **DCO**: siglas para Device Configuration Overlay. Espacio en los discos duros diseñado para almacenar información sobre el fabricante del dispositivo.
15. **DDoS**: siglas en inglés para Denegación de Servicio Distribuido. Es un tipo de ataque en el que se utilizan diferentes equipos para hacer muchas peticiones a un recurso con el fin de bloquear las peticiones legítimas.
16. **DumpIt**: herramienta desarrollada por Moonsols que permite copiar la información almacenada en memoria RAM a un archivo.

17. **Evidencia digital**: elemento de información que por su contexto puede ser considerada para ofrecer certeza clara y manifiesta de un evento ocurrido en un sistema de información.
18. **Firma hash**: cadena de longitud fija producto resultante de la aplicación de una función matemática irreversible a una cadena de longitud variable
19. **FTK Imager**: programa desarrollado por AccesData que permite realizar imágenes forenses desde diferentes medios.
20. **Hactivista**: grupo de personas organizadas que realiza protestas a través de Internet, realizando ataques a sitios web de organizaciones con ideales contrarios a los suyos.
21. **HPA**: siglas para Host Protected Area. Espacio en los discos duros diseñado para almacenar información sobre el fabricante del dispositivo.
22. **Imagen forense**: copia bit a bit del contenido de un dispositivo de almacenamiento.
23. **Ingeniería social**: conjunto de técnicas verbales utilizadas para obtener información por medio de adulación, intimidación o engaños.
24. **ISP**: Proveedor de Servicio de Internet.
25. **Keylogger**: dispositivo físico o programa diseñado para registrar todas interacciones de un usuario con un dispositivo de entrada, como un teclado.
26. **Malware**: cualquier software malicioso.
27. **Man-in-the-middle**: ataque en el que un intruso es capaz de leer, insertar y modificar mensajes en una comunicación entre dos partes sin que estas se den cuenta de la presencia del intruso.
28. **Phishing**: acción de intentar obtener credenciales de acceso o información personal de usuarios de algún servicio utilizando la imagen de una entidad conocida, como un banco o red social.
29. **Plugin**: programa que realizan una función complementaria para otro programa.
30. **Process Explorer**: programa desarrollado por Sysinternals para listar los procesos en ejecución en un sistema Windows.
31. **PSTViewer Pro 4**: programa desarrollado por Encryptomatic LLC que permite administrar contenidos de Microsoft Outlook.
32. **Robo de identidad**: uso de datos personales legítimos de una persona para apropiarse de su identidad y realizar actividades fraudulentas.
33. **Script**: conjunto de instrucciones que se ejecutan secuencialmente. Programa.
34. **SHA1**: siglas en ingles para Algoritmo de Hash Seguro. Segunda versión del algoritmo desarrollado por la Agencia de Seguridad Nacional de Estados Unidos y publicado por el Instituto Nacional de Estándares y Tecnología

35. **SQL injection**: ataque a bases de datos que aprovecha la falta de validación de datos de entrada en un sistema para hacer consultas sintácticamente válidas que pueden arrojar información sobre la base de datos y su contenido.
36. **SQLiteManager**: programa desarrollado por sqlabs que permite interpretar archivos sqlite y realizar consultas a estos.
37. **Sysinternals**: subdivisión de Microsoft encargada del desarrollo de utilidades para los sistemas operativos Windows
38. **TCPView**: programa desarrollado por Sysinternals que lista el estado de conexiones puertos abiertos para sistemas Windows.
39. **Triada de la información**: concepto de seguridad de la información que contempla la Confidencialidad, Disponibilidad e Integridad de la información.
40. **Troyano**: programa malicioso embebido en un programa aparentemente legítimo y útil.
41. **Volatility**: conjunto de herramientas de código abierto diseñadas para la interpretación de archivos de volcado de memoria.
42. **Volcado de memoria**: proceso de copia de la información almacenada en memoria RAM a un archivo.

Bibliografía y referencias de Internet.

Bibliografía

- Cano, Jeimy. Introducción a la informática forense. 2da Ed. 2009 Pág. 65 y 66
- Tanenbaum, Andrew S. Redes de Computadoras. 5ta ed. 2012 Pág. 16
- Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. Diccionario jurídico mexicano, Tomo III. México 1983. Pág. 62
- Consejo de Europa, Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001. Pág. 2, Págs. 4-8
- Código Penal Federal. Última reforma publicada en el Diario Oficial de la Federación el 14 de marzo de 2013. Título noveno, Capítulo I Artículos 210, 211, 211 bis, Capítulo II Artículo 211 bis 1-7.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares, Artículo 3 fracción V y VI, Artículo 30.
- Ley Federal del Derecho de Autor. Última reforma publicada en el Diario Oficial de la Federación el 10 de junio de 2013.
- Instituto Nacional de Estadística y Geografía. Censo económico 2009, Estratificación de establecimientos. Micro, pequeña, mediana y gran empresa.
- Asociación Mexicana de Internet. Hábitos de los usuarios en internet en México, Mayo 2012.
- Symantec, Informe sobre Amenazas a la Seguridad en Internet, Volumen 18. Abril 2013

Referencias de internet, consultado en marzo de 2014.

- AMIPCI. Hábitos de los usuarios de Internet en México http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=115&Type=1
- b:Secure. 24 de septiembre de 2012.La importancia de la evidencia y el análisis forense digital. http://www.bsecure.com.mx/opinion/la-importancia-de-la-evidencia-y-el-analisis-forense-digital/
- b:Secure. La mitad de las empresas acusan a su competencia de lanzar ataques DDoS contra ellos, 25 de julio de 2012. http://www.bsecure.com.mx/featured/la-mitad-de-las-empresas-acusan-a-su-competencia-de-los-ataques-ddos-recibidos/
- Consejo de Europa, Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF
- Domaintools. Domain and IP Whois Lookup Tool. http://whois.domaintools.com
- Foxton Software. Herramientas FoxAnalysis y ChromeAnalysis. http://forensic-software.co.uk/
- INEGI. Número de usuarios de Internet en México, abril 2013. http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tinf204&s=est&c=19437
- Microsoft. Soporte para Windows XP. http://support.microsoft.com/kb/314865/es
- Microsoft. Windows Sysinternals, Strings. http://technet.microsoft.com/en-us/sysinternals/bb897439
- Mozilla. Profile folder – Firefox. http://kb.mozillazine.org/Profile_folder_-_Firefox
- Net Market Share. Distribución de sistemas operativos de escritorio en el mercado.

http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpstick=0&qptimeframe=Q

- Net Market Share. Metodología utilizada para generación de estadísticas. http://marketshare.hitslink.com/faq.aspx#Methodology
- Net Market Share. Sitio dedicado a realizar estadísticas de tecnología de Internet. http://marketshare.hitslink.com/
- Nirsoft. MozillaHistoryView v1.52. http://www.nirsoft.net/utils/mozilla_history_view.html
- Real Academia Española. Definición de Informática. http://buscon.rae.es/drae/srv/search?id=ocjtBXu23DXX2NP3hD2G|hsCL4byQmDXX2WsUSTHF
- Real Academia Española. Definición de metodología. http://lema.rae.es/drae/?val=metodolog%C3%ADa
- SANS DFIR. Blog: SANS Digital Forensics and Incident Response. http://computer-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/
- Semiocast. Twitter reaches half a billion accounts More than 140 millions in the U.S. http://semiocast.com/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US
- StatCounter. Metodología utilizada para generación de estadísticas. http://gs.statcounter.com/faq#methodology
- StatCounter. Sitio que permite analizar el tráfico en un sitio web. http://gs.statcounter.com/about
- StatCounter. Top 7 de uso de sistemas operativos en el periodo marzo 2013 - febrero 2014. http://gs.statcounter.com/#os-ww-monthly-201303-201402-bar
- TecnoVirus. Imagen de un keylogger físico. http://www.tecnovirus.com/blog/wp-content/uploads/2012/07/Keyloggers.jpg

- Veracruzanos.info. Aumentó el robo de identidad en Veracruz 25%: Condusef, 3 de agosto de 2012. http://www.veracruzanos.info/aumento-robo-de-identidad-en-veracruz-25-condusef/